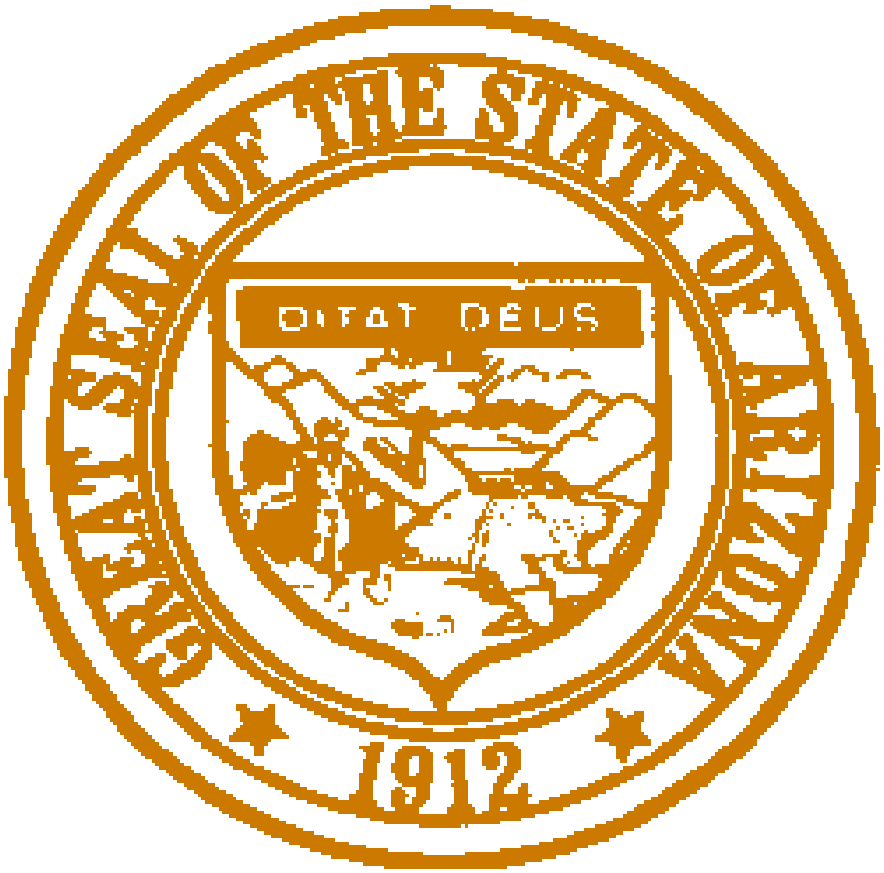
An Information Technology Security Architecture for the State of Arizona



FINAL DRAFT

Prepared By:
The Arizona Department of Administration
John McDowell, Chief Technology Planner
Version 1.2

Table of Contents

Executive Summary

The Security Architecture is an integral and critical component within the overall Enterprise Architecture designed specifically to:

- Enable secure communications and the appropriate protection of information resources within the State of Arizona.
- Support the legal information security requirements established by existing Federal and State statutes pertaining to information confidentiality, accessibility, availability and integrity.
- Support secure, efficient transaction of business and delivery of services.
- Leverage opportunities to obtain IT security synergies and economies of scale.

Accordingly, the Security Architecture supports the overarching goal of Enterprise Architecture to enable and accelerate the development of effective digital government within Arizona by providing a consistent framework that aligns information technology resources with business strategies, and fosters effective and timely technical decision-making.

Observing current trends in both technology uses and abuses highlights the relative significance of the Security Architecture. For example, the number of DNS hosts on the Internet grew from approximately 30 million in 1998 to 110 million in 2001. Over that same time frame, the Federally sponsored Computer Emergency Response Team (CERT) reported a ten-fold increase in security incidents; while information complied from the FBI and Computer Security Institute indicates that:

- 90% of organizations detect some form of information technology security breach.
- 70% of information technology security breaches involve theft of information, financial fraud, or the sabotage of networks or data.
- 71% of organizations experience attacks from insiders, and 59% via the Internet.
- Computer based financial fraud results in $1 million in losses on average.

Three external market factors currently fuel these national trends:

- Latent and immature IT security policy, lay and industry standards
- A shortage of personnel with security technology expertise and experience
- Engineering for “ease of use” has not been matched by engineering for “ease of security”

The information, application, and infrastructure layers of the overall technical architecture are all vulnerable to attack both internally and externally. The following Security Architecture has been developed as a draft guideline for addressing these security challenges and technology opportunities, while pursuing the State’s mission of quality service to its citizens. It provides a framework for consistency, coordination and collaboration in applying security safeguards across the agencies of the State. At the same time, it provides agencies the latitude to use risk-based decision-making processes to determine the appropriate level of protection and product types to be used for obtaining compliance to security policies. The Security Architecture is segmented into distinct components made up of services and technologies. However, each component is not mutually exclusive of the other components.

Implementation of the Security Architecture would require the following actions:

1. The formation and promulgation of a Security Domain Task Team to verify and finalize the recommended standards for each technology in the domain.
2. The publication and enforcement of approved IT Security Policies, Standards, Guidelines and Best Practices by the Government Information Technology Agency.
3. The on-going development and administration of Security Programs by Agencies as directed by the published GITA PSPs.
4. The creation and staffing of a Centralized IT Security Organization which would provide the following services to Agencies:

Service Name	Description
Identification	The process of distinguishing one user from all others
Authentication	The process of verifying the identity of a user
Authorization and Access Control	The means of establishing and enforcing user rights and privileges
Administration	The process of establishing, managing and maintaining security functions and activities
Auditing	The process of monitoring the identification, authentication, authorization and access control, and administration to determine if proper security has been established and maintained.

The deployment of the Security Architecture with the centralized support organization carrying out its related services best positions the State of Arizona to:

- Promote ease and quality of security engineering across the enterprise (State)
- Leverage the State's limited resource pool and budget
- Prevent fragmentation when applying security technology and practices within agencies
- Allow for the rapid response to both technology opportunities and to security threats
- Enable the State to take advantage of, adjust to, and/or influence the direction of industry security practices, standards, technology, and legislation.

1.0 Introduction and Background:

There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order to things. – Niccolo Machiavelli

As the United States progresses from an industrial to an information based society, the importance and value of the State of Arizona's information resources becomes increasingly evident. The potential for constructive use, and possible abuse, of Arizona 's information assets grows exponentially with the vast increase in the amount of data collected and the development of increasingly effective systems for processing it. However, the State has yet to fully accommodate the realities of an information intensive future in its architecture, processes and investments. Technology has continued to evolve and the problems have become much more difficult and complex. Government must now accomplish more than anyone could have imagined five years ago when every one started to focus on "fixing the Y2K problem". Perhaps even more important is the dawning realization that incremental modification to our existing institutions and processes will not produce the adaptation that is needed.

The reality seems compelling. At some future point in time, the United States, along with Arizona, will be attacked, not by hackers, but by a sophisticated adversary using an effective array of information warfare tools and techniques. Two choices are available: adapt before the attacks or afterwards.

The discussion of the proposed security architecture offers a realistic set of options and strategies to adapt before the attacks. It is incumbent of government to properly and efficiently shepherd Arizona 's information assets for the sole benefit of its citizens. To insure the efficient and effective protection of these assets, Arizona IT must provide a consistent clear framework _that gives governmental entities the ability to implement _secure environments for these resources. This document provides a critical piece in this framework, by delineating principles, best practices and standards for security technology within the State of Arizona.

The State must provide quality services to its customers while protecting its assets and resources. It must ensure compliance with legal requirements for confidentiality and privacy while providing public access to appropriate information. Therefore, the State must implement security services in such a manner that its "information infrastructure " is protected while, at the same time, its functionality is unimpeded and its business services are readily available. Further, it is necessary that the cost of security measures be measured against the potential fiscal and legal consequences of security failure.

Security services apply technologies to perform the functions needed to protect assets. Historically, such services have consisted of door locks, vaults, guards, sign-in/sign-out logs, etc. As the State performs more business functions electronically and expands electronic serve to citizens in a more open environment, it opens itself to additional risks. No longer is physical presence a requirement for information attack. Networks once closed are now available globally 24 hours a day. As the electronic age transitions from closed, proprietary systems to more open distributed systems, additional security services will be needed to protect the State 's information infrastructure. For example, depending of the data protected, the use of simple electronic passwords within a SNA network may require biometrics-based identification methods when opened to the Internet.

A specific example of progress coming hand-in-hand with new vulnerabilities is the State's embrace of Web-based technologies, which offer great flexibility and ease of operation. On the other hand, the concomitant vulnerabilities of such an approach mean that defensive security measures have never been more important than at the present time.

Arizona State Government is developing closer electronic partnerships with businesses outside of state government, some employees are mobile users, some employees are working from their homes, and state services are being brought closer to the citizen electronically. The purpose of security is to protect and secure the State's information resources in order to provide an environment in which the State's business can be safely transacted.

A directory is a natural place to centralize management of security. It is the vault that contains the most trusted and critical components of an enterprise security strategy. This will require authorization and authentication services and a common enterprise repository of digital certificates that secures and supports E-commerce applications. Security services apply technologies to perform the functions needed to protect assets. Historically, such services have consisted of door locks, vaults, guards, sign-in/sign-out logs, etc. As the State performs more business functions electronically, it must transition to security services designed to protect the electronic environment. For example, the use of face-to-face identification must be superceded by an equivalent electronic method that does not require the physical presence of the person.

Figure 1 - Compares traditional business methods to electronic business methods.

Traditional Business Versions	Electronic Business Versions
Handwritten signatures	Digital signatures
Visual identification of individuals and business partners	Biometrics, smart cards, token cards, Public Key Certificates
Notary services	Digital time stamping and digital signatures
Visual inspection of documents to detect modifications	Integrity and cryptography services

As the electronic age transitions from closed, proprietary systems to more open, distributed systems, additional security services will be needed to provide protection in a dynamic and less controllable environment. For example, the use of simple electronic passwords within a local network might be supplemented by biometrics-based identification methods when used across the Internet. Therefore, the State must create a security architecture that will provide the strategies and framework necessary to protect its information infrastructure while it transacts business in a changing electronic world.

1.1 Enterprise Architecture Model

GITA has created an Enterprise Architecture for the State of Arizona with the following three purposes:

1. Establishes a Statewide roadmap of technology to achieve its mission of core business processes for State benefits and services within an efficient IT environment.
2. A Blueprint for defining the State's current technologies (baseline) and desired technologies (target) environment.
3. EA's are essential for evolving information systems, developing new systems, and the insertion of emerging technologies that optimize their mission and value.

The following ten general principles provide the framework for defining the baseline and target architectures within the technical domains:

1. Architectures must be appropriately scoped, planned, and defined based on the intended use of the architecture.
2. Architectures must be compliant with the law as expressed by legislative mandates, executive orders, State and Federal regulations.
3. Architectures facilitate change.
4. Enterprise architectures must reflect the Governor's Strategic Plan, The Statewide IT Strategic Plan and the Agency's Three-year IT Plan.
5. Architectures continuously change and require transition.
6. Target architectures should project no more than 3 to 5 years in the future.
7. Architectures provide for a standardization of business processes and common operating IT environments.
8. Architecture products are only as good as the data collected from subject matter experts and domain owners.
9. Architectures minimize the burden of data collection, streamline data storage, and enhance data access.
10. Target architectures are used to control the growth of technical diversity.

GITA has defined a technology layering approach to the Enterprise Architecture with five basic domains.

- **Network Architecture:** Defines the State's communications infrastructure, which includes the various topologies, transmission services and protocols necessary to facilitate the interconnection of server platforms, mainframes, intra-building and office networks (LANs), and inter-building and mall/campus networks (WANs).
- **Platform Architecture:** Identifies computer hardware devices, which include client and server platforms, mainframes, mid-size computers, workstations and desktop microcomputers.
- **Security Architecture:** Identifies security technologies, policies and standards necessary to protect the information assets of the State and to provide various information layers available to the State's workforce and citizens as appropriate. The objective of this architecture is to ensure confidentiality of information, integrity of data, and the availability of IT resources.
- **Software Architecture:** Defines software policies and standards of operating systems, program source code, compilers, database management products, etc.
- **Data/Information Architecture:** Identifies the organization of information related to citizens, locations and objects the State must collect, store, maintain, and access. This layer of architecture will improve the business process to business intelligence to help ensure that State services are executed in a timely, efficient and cost-effective manner.

The subject of this document is the Security Architecture domain for the State of Arizona. To be consistent with Enterprise Architecture Principle 4 above, the proposed security domain will meet the planning compliance criteria in the following manner:

- The three security goals to be achieved are: 1) Confidentiality, 2) Integrity, and 3) Access. These 3 goals will support all five of the GITA Statewide IT Goals documented in the "Statewide Information Technology Vision And Strategic Direction for Fiscal Year 2002 and 2003". In fact, none of these goals can be achieved if IT security is lacking. Specific

correlation documentation will be prepared in a future release of this section. The five GITA goals are:

1. Increase the use of e-government solutions.
2. Effectively share common IT resources to enable State agencies to better serve the people of Arizona.
3. Improve access to broadband infrastructure Statewide.
4. Improve cross-agency applications integration and data sharing along with the quality, efficiency, and usefulness of electronic information.
5. Improve the capability of IT functions in order to deliver quality products and services.

- The purpose of the security architecture is to create the proper framework for protecting the State's IT assets. This is in support of the Governor's goal 16… "Deliver Courteous, Efficient, Responsive, and Cost-Effective Service to Citizen Owners and Employees of State Government".

1.2 Today's IT Security Threat Environment

"He that will not apply new remedies must expect new evils" - Francis Bacon

The American Homeland is becoming increasingly vulnerable to non-traditional attack, including information systems attacks. Rapid advances in technology capability have and will continue to create new challenges to our security. During the early phases of Y2K over 250 mission critical applications were identified and remediated. New commercial off-the-shelf (COTS) applications are implemented on a regular basis, and although some positive testing is conducted to determine if the software will perform as expected, virtually no negative testing is done to determine what unanticipated vulnerabilities may be imbedded in the software. Major products and operating systems are known to have vulnerabilities that expose the users to new risks.

Recent studies, by both the Government Accounting Office and the Computer Security Institute found that the number of cyber security threats to both the government and the private sector is on the rise. The damage to both the physical infrastructure and the psychological health of US institutions could prove immense by a successful attack, and the State of Arizona is not exempt from this danger.

There is a growing lack of confidence in the information network as well as in the integrity of the data contained therein. The information warfare threat applies to systems everywhere. A perimeter defense philosophy is currently the predominant solution across the State. The problem with this approach is that it leads to a strategy of risk avoidance rather than risk management. Perimeter defense does not equal defense-in-depth. Perimeter defense relies on an outer barrier that is intended to prevent unauthorized access to a network. Once the barriers are in place authorized users must be given access – usually through passwords or other identifiers. As work progresses, secondary users are often identified and granted access on a temporary basis, or restricted to specific levels of data. Finally, due to operational need and convenience still others are granted access. The end result is a network that started out with the expectation of security, and ended up with no clear idea of who is really in the network. This "Swiss cheese effect" is a nightmare for network security personnel, as intruders gain access through stolen passwords, backdoors, data manipulation, and corruption of the system.

Defense-in-depth security uses a layered approach with multiple firewalls, intrusion detection devices, and network security tools. As intrusions are detected, intruders can be shut down, denied further access, tracked for future legal action, and/or counterattacked. There are at least

three layers: 1) prevention, 2) detection, and 3) tolerance. The tolerance level represents those intrusions that may be unavoidable – often the insider threat. These are threats that must be managed. Consequence management requires back-up systems, redundancy, heightened awareness, integrity restoration, and recovery and reconstitution. These are the keys to graceful degradation rather than catastrophic failure.

In order to protect its resources, the State must first assess the types of threats that it will encounter relative to its information infrastructure. It must understand the forms of threats that are possible in the electronic technology environment and it must determine what impact any particular threat will have on the State's business.

Figure 2 – Shows the generic types of threats and their impact on the State's information technology assets.

Type of Threat	Description	Form of Threat	Impact
Modification of data in transit	Modification of transactions across networks	Exploit weaknesses in communication protocols	Financial losses, Inconsistent data
Denial of Service	Attacks which bring down servers or networks	Exploit weaknesses in communications protocols and operating systems	Prevent the State from transacting business
Theft of Information	Penetration attacks resulting in theft of information	Exploit security weaknesses in applications, operating systems and host machines	Legal and regulatory requirements to maintain confidentiality
Unauthorized use of resources	Penetration of systems can allow attacker to utilize services such as computers phones services	Exploit weaknesses in applications, operating systems and host machines	Financial loss Potential Liability (Lack of due diligence) Compromise state systems
Data Tampering	Modification of State data, pages, such as health records, student transcripts, driving records, etc.	Exploit security weaknesses on server to modify Web pages, contents of databases	Impact to State Image Falsification of information can have damaging consequences
Spoofing	Impersonating an internal address to achieve access Impersonating others in email	Exploit communication protocol weaknesses allow attackers to impersonate others	Access can result in compromise or damage to State systems Impact on State image
Sniffing	Monitoring Network traffic for information including passwords	Network traffic is transmitted in clear text, passwords and data can be recovered	Access can result in compromise or damage of State systems
Viruses Vandals	Malicious programs including component based applets which range from harmful to harmless	Ease of Downloading software	Added business expense and lost productivity
Physical destruction of infrastructure, systems and / or data	Attacks which physically destroy the asset so that it must be replaced before service can continue	Attacker exploits vulnerabilities with intent to inflict permanent destruction or harm to the assets of the organization	Prevent the State from transacting business

2.0 An Effective Security – Information Assurance Architecture

2.1 Summary

The Integrated Information Infrastructure (III) and State Information Grid (SIG) concepts come from the new Federal Homeland Security Agency and the Department of Defense at the national level. These concepts are presented for consideration as part of the State of Arizona IT Security Architecture.

An Integrated Information Infrastructure (III), a vision currently being developed for the State, can be the foundation on which many of the information infrastructure initiatives can be based. The III sets goals and directions for Statewide information services that will be developed from private-sector information technologies.

The first phase in the realization of the III will be the implementation of the State Information Grid (SIG). The SIG will interconnect information capabilities, automated processes and personnel for collecting, storing, processing, managing and disseminating information on demand to citizens, policy makers, other government entities and private sector business partners involved in the State's business of serving citizens.

The SIG will comprise multiple virtual private networks Statewide that use shared commercial communications media and information technologies. However, the State will not own or control the SIG. Furthermore, the SIG will offer virtually no protection against insider threats, especially to tactical networks. No centralized authority over budgets and execution activities exists today. A new organizational structure with a centralized shared services primary point of responsibility is needed.

It is recommended that an information assurance (IA) reference model that assumes the use of Internet protocols in a wide range of environments (including tactical and strategic) be established. It will parallel the International Organization of Standardization (ISO) reference model, with the substitution of a middleware layer for the presentation layer, and is consistent with the Transmission Control Protocol/Internet Protocol (TCP/IP) Suite. It is further suggested that the following strategies be considered:

- The use of a consistent architectural framework and metrics across the entire SIG.
- Segmentation of the user communities and investment in Public Key Infrastructure (PKI) and Public Key Enabled Applications (PKE) as well as high-speed, in-line encryption.
- The establishment of a Statewide SIG IA Testbed.

In particular, it is recommended the following measures to support IA over the SIG:

- A uniform layered-defense, or defense in depth (DID) architecture
- IA functions in the host computers and servers of the SIG, including host-based intrusion detection and response, end-to-end security, domain name system security and malicious and mobile code eradication.
- Secure network management capabilities
- Adoption of PKI / PKE
- Link encryption at the physical layer
- An ISO-like reference model with commercial protocols (e.g., Internet Protocol security (IPsec) for end-to-end protection)
- Fine-grained control of access to computers and communications resources

- Features to counter insider attacks and support survivability
- Features to counter denial of service attacks
- Measures of merit or metrics for IA and survivable architectures, for technical, system and mission-level evaluation

Other recommendations include the use of correlated multi-layered Intrusion Detection System (IDS) data as inputs to intelligence-enabled tracing systems and modus operandi detectors.

2.2 The Integrated Information Infrastructure

The Integrated Information Infrastructure (III) vision sets goals and direction for Statewide information services that will come about through the exploitation of private sector IT, to include associated information assurance technologies. The III then sets both a long-term vision and a road map for the evolution of the State's infrastructure.

To realize the potential benefit of this concept, the future information infrastructure must be capable of reliable, secure transmission, storage, retrieval and management of large amounts of data. Today, all systems are segmented into communications links, computers and sensors that in turn are stove-piped to support specific functions. Furthermore, these component entities are now constrained by a lack of: (1) the bandwidth necessary for high-speed, high-resolution image transfer; (2) memory sufficient to handle massive amounts of archival data; (3) lack of software and repositories to search the many files and databases in a timely manner. These constraints are magnified by difficulties in integrating a myriad of legacy information systems with newly developed, agency-unique stove-piped and joint systems. These limitations can be overcome and a full capability of seamless integrated services delivered through a ubiquitous, flexible, interoperable system of systems – the Integrated Information Infrastructure.

The infrastructure must allow information to be distributed to and from any source or user of information at any time: its architecture must not be constrained to support a force-structure enterprise hierarchy conceived a priori. Most importantly, the information and services provided to the end-user through the infrastructure must be tailored to the user's needs, and be relevant to the user's mission, without requiring the user to sort through volumes of data or images.

The information infrastructure must include multi-mode data transport including landline, wireless, and space-based elements. All of these media must be integrated into a ubiquitous, store-and-forward data internetwork that dynamically routes information from sources to destinations, transparently to the user. This data transport segment of the infrastructure must be self-managed, be adaptive to node and link failure, and provide services to its users based on quality of service requests. These services include bandwidths, latency, reliability, security, precedence, distribution mechanisms (point to point and point to multiple point), and the like.

The infrastructure should be an adaptive entity that integrates communications systems, computers and information management resources into an intelligent system of systems. Each component of the III will exchange State information with each other, in order to enable the entire infrastructure to adapt to user requirements and any stresses imposed on the network by an adversary. This adaptability will also enable the infrastructure to change its scale as necessary to incorporate new processing, network, and communication technologies as they are developed. Thus, this infrastructure is a scaleable computing environment.

To the maximum extent feasible, the infrastructure's transport layer will take advantage of commercial technology and networks, by utilizing open-systems standards and protocols, and will minimize the use of service or function-unique hardware and software.

2.3 The State Information Grid

The first phase for realizing the III is the implementation of the State Information Grid (SIG). The SIG will incorporate near-term information technologies to provide the capabilities noted above. The SIG will, over time, evolve into the longer-term vision for the III. As the State proceeds to implement and secure the SIG, it must keep the evolution toward the III in focus.

Today's communications infrastructure is highly entwined, with many misunderstood capabilities and limitations – and a false sense of security. Long-haul communications are one clear example. Multiple users may think they have a "unique circuit", when in fact they are only sharing a fiber or a part of a larger fiber optic cable. Assumptions of privacy, dependability, and assured service are often faulty. In most cases, these long-haul communications merge into a distribution switch that further routes the signal to its destination – making the switch a potential single point of failure.

State Information Grid

Definition
State interconnected information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to citizens, policy makers, government entities and business stakeholders.

The SIG includes:
All owned and leased communications, computing systems and services, software, applications and security services

The SIG supports:
All branches of State Government

The SIG provides capabilities from all operating locations:
Agencies, boards, commissions, schools, courts, facilities, mobile platforms

The SIG provides interfaces to:
federal government, local government, citizens, businesses

2.4 Security – Information Assurance Architecture

The State Information Grid (SIG) will comprise multiple virtual data networks, the Non secure Internet Protocol Routed Network (NIPRNET), Secure Internet Protocol Routed Network (SIPRNET), Arizona Government MAGNET, and individual agency command, control, applications and systems as presently constituted. These networks use shared commercial communications media and commercial information technologies. In addition, all are cryptographically segmented into virtual networks. However, there is very limited capability deployed against insider threats to security. At the present time each entity is using their own "defense-in-depth" (DiD) strategy (or lack thereof). While there is a general framework for implementing DiD, there is no engineering discipline that allows for design of a DiD solution that provides confidence in security against a variety of attacks.

The current emphasis on information assurance metrics is a focused on readiness and is not addressing the metrics needed to assess and measure mission, strategic, system and or technical level performance. In addition, denial of service measures and metrics are not well addressed.

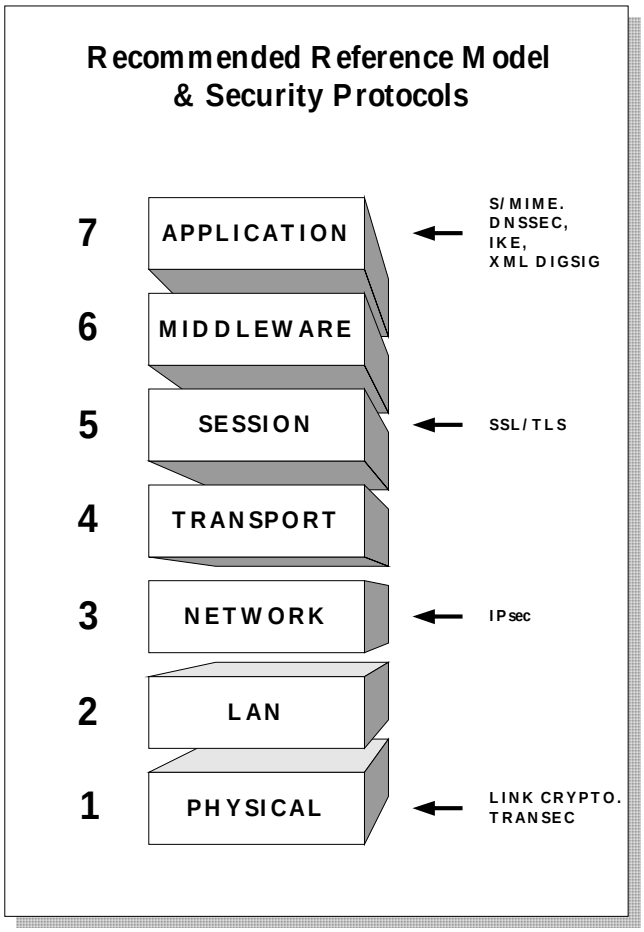
SIG IA: Summary of Findings

- SIG today = NIPRNET + SIPRNET + MAGNET + Agency Tactical Systems
  - All transit commercial communication media
  - All leveraging commercial IT
  - Insider threat not addressed
  - All crytographically segmented into virtual networks
- Multiple efforts causing some confusion and misdirection
- Rigorous, consistent defense-in-depth not occurring
- Immature IA metrics
- Denial of Service Attacks not well addressed
- Mobile code still an issue, but critical to future technology

There is currently no office of primary responsibility for broad shared IT infrastructure and security. Without development of such a function the vision of III and SIG can not and will not occur.

2.5 Information Assurance Reference Model

The information Assurance reference model that is suggested is shown below. This protocol stack assumes the use of Internet protocols in a wide range of environments, including both tactical and strategic. It parallels the International Organization of Standardization (ISO) reference model (ISO 7498), with the substitution of a "middleware" layer in lieu of the presentation layer, and is consistent with the TCP/IP suite. This substitution seems appropriate because most modern systems do not make use of the separate presentation layer functions; these functions are assumed by applications.



In this model, physical layer protection is afforded via link KGs on a hop-by-hop basis, where warranted by threat concerns. No data link security is recommended because of lack of vendors uniformly adopting such standards as IEEE 802.10. Internet Protocol security (IPsec) is recommended for end-to-end, enclave-to-enclave, or end-to-enclave protection. NO transport (e.g. TCP) layer security protocol is recommended because there are no widely used standards yet available, and because the services provided at the IP and session layers obviate the need for transport layer security.

Although the Internet protocol stack does not include a session layer per se, the introduction of Secure Socket Layer (SSL), Secure Shell (SSH), and analogous security protocols has created one. SSL is widely deployed and general policy calls for its use for secure web access.

The insertion of a "middleware" layer is suggested to accommodate systems such as Common Object Request Broker Architecture (COBRA), distributed computing environment (DCE), or Enterprise Java Beans (EJB). However, such systems are not universally required and there is no clear appropriate choice among these competing middleware technologies at this time. Finally, several critical protocols exist at the application layer, and more may emerge. For secure e-mail, S/MIME (v3 with enhanced security services) is the preferred protocol, and it is widely available in Commercial Off-the-Shelf (COTS) products. Secure Domain Name System (DNS) is an essential infrastructure security component requiring further consideration. Internet Key Exchange (IKE) is the key management protocol used by IPsec. As Extensible Markup Language (XML) becomes more common, the digital signature standards developed for it will become critical elements of more sophisticated web security designs, supplementing, but not supplanting, SSL/TLS.

2.6 Information Assurance / Security Architecture Strategies

The following table summarizes several strategies that the State should use in deploying a consistent security architecture for its technology systems.

Information Assurance Strategies

- Discipline Implementation
  - Use consistent architectural framework and metrics
  - Ensure interoperability via commercial standards
- Segment the Communities of Users
  - State vs. General Public, by classifications, by enclave COI, by user authorization within enclave
  - Invest in PKI / PKE & high speed, inline IP encryption
- Counter Denial of Service
  - Use segmentation, redundancy, diversity, restricted set of Internet access points, & non-switched commercial infrastructure
  - Improve net infrastructure security (e.g., Secure Boundary Gateway Protocol)
- Enhance Indicators and Warnings
  - Correlate multi-layered IDS outputs, use as inputs to
    - Intelligence-enabled tracing systems
    - Modus operandi detection
  - Use PKI to increase S/N ratio
- Establish a State-wide Information Assurance Testbed

Discipline Implementation - The first strategy is to use a consistent architecture framework and consistent metrics across the entire SIG. This strategy contrasts the current divergence of approaches by the several agencies. It is important to foster interoperability via commercially available standards, so that commercial and government off-the-shelf technology can be employed throughout the system.

Segment the Communities of Users - The defense-in-depth approach leads to the strategy of segmentation. Segmentation is recommended between the State government to government access and data sharing, and the access by the general public through the Internet. In order to support segmentation, investment will be needed in high-speed in-line IP encryption devices and in large scale PKI and PKE for specific users and applications as required.

Fine-grained Access Control (FGAC) is the principle that allows access to computing and communications resources to be shared, in a safe manner, among a large number of agencies and agency customers. Technology is available to enforce FGAC with an acceptable level of computational overhead. However, tools must be made available to enable local administrators and users to efficiently manage FGAC for Wide Area Networks, Local Area Networks, and individual hosts and servers.

FGAC is supportive of accountability and acts as a deterrent to inside attacks. Fine-grained identification and authentication provides the inputs needed to make FGAC decisions. Intrusion detection mechanisms help detect attacks that have eluded access controls, or activities that represent inappropriate use of resources by authorized personnel.

Counter Denial of Service - The third strategy is intended to counter denial of service. Segmentation, redundancy, diversity, a restricted set of Internet access points, non-switched commercial infrastructure, and improved overall net infrastructure security, such as S-BGP used in concert can partially mitigate the denial-of-service threat.

Enhance Indicators and Warnings - Another important element of the overall strategy is to enhance indicators and warnings. This leads to the fourth component. By correlating multi-layer intrusion detection system outputs, one can detect patterns of behavior that may indicate a modus operandi. This information can be useful in tracing the sources of unwanted behavior. The correlated outputs of host and networked-based IDS at various levels can also be used to direct attention to potential threats. Resources such as human system administrators and various intelligence assets can be directed in this way.

Establish a Statewide Information Assurance Testbed - The last strategy is to establish a Statewide information assurance test-bed. This test-bed would draw red and blue team members and current configurations information from the SIG operations. The lessons learned through these exercises should be used to upgrade the IA properties of the test-bed, and if successful in defense, should be transitioned to the operational SIG. Building and IA test-bed avoids the costs and other issues inherent in red teaming with the live SIG.

The State should develop a deep understanding of how commercial services are provided, so that they can be properly specified when purchased. For example, buying communications lines from multiple suppliers in order to gain redundancy and diversity may not yield the desired results, if each supplier's fiber goes through the same physical switch or runs over the same physical bridge. Instead, when buying a second communications line, the State should specify that the line shares no physical components or transit mechanisms with the first communication line.

3.0 Security Architecture Design Principles

The following principles apply to the enterprise security architecture. Enterprise principles are relevant to both Statewide and specific individual agency information infrastructures.

Principle 1: Security levels applied to resources should be commensurate to their value to the organization and sufficient to contain risk to an acceptable level.
Security is a business enabler with associated costs. Security costs should be rationalized to the intended benefits.

Rationale:
- Requirements for security vary depending on the information system, the type and number of connections to other systems, the sensitivity of data, and the probability of harm.
- Each type of transaction will have individual security requirements.
- Security costs can increase beyond the value of the assets being protected. Do not use more security than is required.

Principle 2: The architecture must accommodate varying security needs.
Varying levels of protection are supported without modifications to the security architecture.

Rationale:
- Requirements for security vary depending upon the nature of communications, the sensitivity of the information, and the risks to the enterprise.
- Requirements for security vary within and between different Agencies.
- Security needs change.
- Security services must be granular enough to accommodate the different levels of assurance required, and extensible enough to meet future needs.

Principle 3: The architecture must provide integrated security services to enable the enterprise to conduct safe and secure business electronically.
Arizona must be able to conduct business electronically while maintaining information availability, confidentiality, and integrity.

Rationale:
- Arizona will continue to increase the volume of business conducted electronically. These transactions must be safe and secure.
- Providing integrated security services enables the growth of electronic business.

Principle 4: A single, accurate and consistent system date and time should be maintained across the enterprise.
A single, accurate, and consistent date and time are essential to all security functions and accountability.

Rationale:
- The validity of digital signatures and electronic transactions depend on precise, accurate, and reliable date and time information.
- Audit accountability relies upon placing events sequentially according to date and time.

3.1 Security Component Principles

Security Domain Principles represent the fundamental concepts that provide the foundation for the standards, best practices, and implementation guidelines, which compose the Security Architecture Components.

1) The Security Domain Definition Team endorses and supports the Conceptual Architecture Principles identified by GITA in the "Enterprise Architecture Model" and deems them applicable to the Security Architecture ***as qualified*** in Item 2 below.

2) The Security Domain Definition Team has further identified the following domain specific principles, which provide additional structure for the Security Architecture Components, and which further qualify the Conceptual Architecture Principles from a security perspective. The Security Architecture Components must:

    - facilitate proper and efficient security identification, authentication, authorization, administration and audibility in response to the access and use of information resources

    - support and remain compliant with State laws and Federal regulations (e.g., H.I.P.A.A and Rehabilitation Act, Sec. 508) with respect to security, privacy, availability, accessibility, etc

    - provide for portability across platforms and utilize Open Standards at all levels

    - support multiple service delivery channels where feasible

    - ensure that security requirements and associated risks are adequately evaluated when preparing to support adaptability, availability, access, data capture and data sharing needs of the state

    - be flexible to support the introduction and/or integration of new technologies, while maintaining appropriate security protection and requirements

    - ensure that the accountability and responsibility of all persons fulfilling security duties are sustainable, assignable, and enforceable

    - address and support multiple layers of protection, including network level, operating system, application level and data level security needs

4.0 General IT Security Best Practices

Best Practice 1: Perform a business driven risk assessment for all automated systems.

- A risk assessment should be performed for all new and ongoing business systems. To determine the appropriate security requirements, business units should assess the value of system assets, risk exposure to those assets and evaluate the costs of protecting those systems.
- Understanding the value of assets and associated risks is essential to determining the level of security required.
- Security requirements should be included when designing or purchasing new applications.

Best Practice 2: Design application security to follow the State security architecture.

- Application security will make use of different technologies to provide security services, but an application 's security should follow the State architecture (5 services).
- Whenever possible, application security should use existing infrastructure security services.
- If existing infrastructure security services cannot be used, application security should take advantage of open standards, or ubiquitous proprietary standards (e.g. RACF) to ensure interoperability.

Best Practice 3: Locate security in the architecture to ensure maximum usability with minimum future modifications.

Whenever security is required, the location in the architecture will have an impact on performance and usability. Choosing the appropriate location will maximize usability while minimizing the need for future modifications.

Best Practice 4: Develop and implement a security awareness program.

- A security awareness program is an important, often overlooked, component to a secure environment. These programs educate the user on security do's and don'ts. Implementing smart cards as an Identification technology will not have the desired effect if the card 's owner loans it (and their PIN) to others.
- Security awareness programs should educate the user community on security policies.

Best Practice 5: Manage security policies centrally.

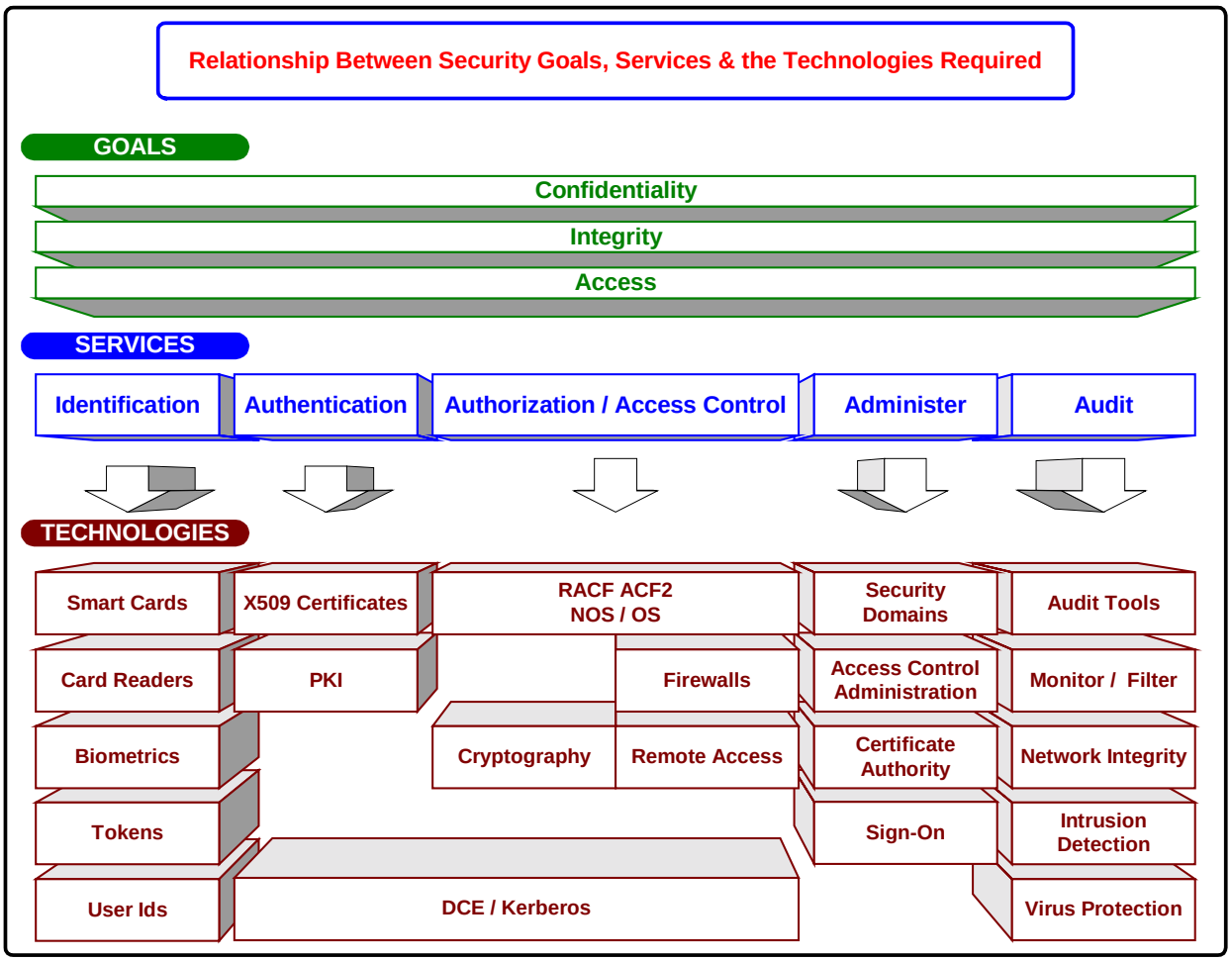
Central management of security policies and implementation provide a single point of accountability and responsibility. Central management does not have to be performed by a single individual. It depends upon the size of the organization and its systems. For a larger organization a group could be responsible with individual members of the group responsible for particular areas.

5.0 Security Goals, Services and Technologies

The following chart shows the relationship between security goals of: 1) maintain confidentiality, 2) ensure integrity of data, systems and infrastructure and, 3) provide ubiquitous and continuous access to resources.

Security will be achieved through a series of five services carried out through sub functions, standards and technologies required to support the three goals. Each of the identified services has a section of the architecture devoted to describing the technology components, the best business practices utilized, and the standards that are deployed in support of the technologies.

The following defines the services at the highest level:



The mission of the State 's security architecture is to provide a framework that ensures the availability, integrity, and confidentiality of Arizona 's information infrastructure, systems and data.

This is accomplished by providing identification, authentication, authorization/access control, administration, and audit security services utilizing component technologies, best practices, guidelines, and standards. Arizona 's security architecture is built upon a foundation of security services, component technologies, best practices, guidelines, and standards. The security services used to protect the State 's information infrastructure are:

Identification – The process of distinguishing one user from all others.

Authentication – The process of verifying the identity of a user.

Authorization and Access Control – The means of establishing and enforcing user rights and privileges.

Administration – The process of establishing, managing, and maintaining security.

Audit – The process of monitoring the identification, authentication, authorization and access control, and administration to determine if proper security has been established and maintained.

Each of these services is delivered by implementing one or more component technologies.

Figure 3 – Outlines the relationship between Arizona security Goals, services provided, & the technologies.

Goal 1 Availability	**Goal 2 Confidentiality**	**Goal 3 Integrity**			**Goals**
Identification	Authentication	Authorization - Access Control	Administer	Audit	**Security Services**
Smart Cards Card Readers Biometrics Tokens User IDs	Passwords X.509 Certificates PKI DCE/Kerberos	RACF, ACF2 NOS/OS Firewalls Remote Access Cryptography	Security Domains Access Control Administration Certificate Authority Sign-On Education & Awareness	Audit Tools Monitor / Filter Network Integrity Intrusion Detection Virus Protection	**Technologies**

It is important to note that the technologies listed here are in flux, where the services and goals remain constant. It is exigent that as new technologies emerge or existing one's mature that they be re-evaluated in light of the principles and goal outlines in this document. These security services are delivered, and their component technologies are implemented, in conjunction with a set of best practice guidelines, and industry standards. In addition to the best practices, guidelines, and standards that have been developed for each individual security service, the State of Arizona has developed the following enterprise-wide security principles and best practices.

6.0 Identification Services

Identification Smart Cards Card Readers Biometrics Tokens User-IDs

6.1 Introduction

Identification is the process of distinguishing one user from all others. Identification techniques provide a means of gaining entry to the State 's resources such as workstations, networks and applications. Identification is closely linked to authentication. Authentication is the process of verifying the identity of a user and is covered in the following section.

The most commonly used form of identification is the user-ID. A user-ID is used in conjunction with a password to identify and authenticate a user. Techniques that improve upon the security of user-IDs and passwords have been developed. These techniques include smart cards, biometrics, and tokens. Several identification techniques can be combined to increase the level of security. Today 's current environment is primarily based on user-ID identification and password authentication.

Personnel Security - Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied appropriately to those personnel working for, or on behalf, of the State.

Personnel Security begins during the Staffing process. Early in the process of defining a position, the responsible supervisor determines the type of computer access that is needed for the position and the sensitivity of that position. Best practices suggest that two general principles should be followed in defining a position - separation of duties and least privilege. Once personnel have been staffed, personnel security safeguards are administered according to the Agency's policy via User Account Management. User Account Management involves: 1) establish the procedures for requesting, issuing, and closing user accounts over the life cycle of personnel events; 2) tracking users and their respective access authorizations; and 3) managing these functions on an on-going basis.

6.2 Identification Technology Components

The technology components for identification are discussed below.

User-ids:
Being identified to the State 's IT resources requires the use of a user-ID. User-IDs and associated passwords for authentication are inexpensive and widely integrated into today's systems.

Proprietary Tokens:
Tokens are physical cards similar to credit cards that work in conjunction with a user-ID to identify a user to the system. They combine something a person knows, such as a password or PIN, with something they possess, a token card. Token cards commonly generate either dynamic passwords or a response in a challenge-response communication between the user and the system. Tokens are commonly used for secure remote access where high levels of security are required. It is likely that tokens will become obsolete and will be replaced by PKI as PKI matures.

Hand Geometry
Hand geometry has features similar to fingerprints, though perhaps a higher social acceptability. Similar devices are used in both cases. Hand geometry is less accurate than fingerprints because of a lower number of features and less variability in these features. It may be acceptable when a user is matched against a known template. It would be less acceptable when trying to match against a large set of templates

Face Geometry
Face geometry uses a standard video camera to capture facial images. The system extracts features that don 't easily change, such as the geometry of the eyes and nose, from the images. The template created is matched against real-time images. People do change, and facial hair, positioning and glasses can affect accuracy. Face geometry is less accurate than fingerprint biometrics.

Fingerprint Biometrics
Fingerprints have traditionally been used as an identification tool in law enforcement. Fingerprint recognition systems convert a scanned image of a fingerprint into a mathematical representation of the features. The main strengths of fingerprint recognition are its long history, the variability in fingerprints, ease of use, cost and accuracy. Additionally it has the potential to be integrated into inexpensive devices such as smart cards and keyboards. A disadvantage may be its social acceptability due to its association with illegal activities.

Biometrics:
A biometric is a unique, measurable physical or behavioral characteristic of a human being. Biometrics is useful for automatically recognizing or verifying identity. Biometric characteristics can include fingerprints, hand and face geometry, signature and voice. Each of these methods has different degrees of accuracy, cost, social acceptability and intrusiveness. An extreme example of an intrusive technique would be a DNA sample. DNA biometrics will not be covered in this section, as it is not a financially or technically viable means of identification to information systems at this time. Voice identification would be an example of a non-intrusive and socially acceptable technique. All biometric products operate in a similar way. First, a system captures a sample of the biometric characteristic during an enrollment process. Unique features are then extracted and converted by the system into a mathematical code. This code is then stored as the biometric template for that person. The template may be stored in the biometric system itself, or in any other form of memory storage, such as a database, a smart card or a barcode. When a user needs to be identified, a real-time sample is taken and matched against stored templates. If the match is within pre-defined tolerances, the individual's identity is established. There is no perfect biometric technique for all uses. Different biometric techniques are more suitable for particular situations. Factors can include the desired security level and the number of users. For instance, identifying a user for access to the State 's systems matches that user to their known biometric template (one-to-one match). This is easier than identifying a welfare applicant from the larger set of existing recipients to reduce duplication of benefits (one-to-many match). Biometric systems are not 100% accurate. Accuracy in biometrics is measured by false acceptances versus false rejections. False acceptances are when an unauthorized user is allowed access. A false rejection is when an authorized user is denied access. Thresholds can be adjusted to reduce one type of error at the expense of increasing the other. The choice of threshold depends on the level of security required, the acceptability of the type of error, and user acceptability. The accuracy of biometrics can also be improved by combining two techniques such as fingerprint identification and face recognition. An intersection of the matches from two biometric techniques typically results in an acceptable identification.

Voice Biometrics
Voice biometrics is based on distinguishing the sound of a human voice based on the resonance of the human vocal tract. It is different from voice recognition, which is recognizing spoken commands or words. The system is trained by repeating a phrase that will be used as an access code. One shortcoming of voice biometrics is false rejects that deny a legitimate user access. This is due to medium to low accuracy rates and dependence on the type of equipment used. It may be suitable for outdoor situations and telephone access.

Signature Recognition
Signature verification depends on the rhythm, relative trajectories, speed, and number of pen touches. It measures the method of signing instead of the finished signature and, therefore is different from the comparison of a signature. A pen-based computer or digitizing pad is required for signature capture during enrollment and during verification. It has a relatively low level of accuracy. It may be acceptable where a history of signature use exists such as retail transactions and document authentication. It has limited uses where a large number of people must be identified in a limited time. It also has the disadvantage of requiring the individual to want to be identified. This limits its use in applications such as welfare or social benefits identification.

Smart Cards & Card Readers:
A smart card is a tamper-resistant computer embedded in a credit card sized card. The cards have embedded integrated circuits that implement a CPU, application data storage and RAM used by the CPU. A smart card and associated host software are used both as an application platform and an identification and authentication device. The smart card as an application platform is covered in the platform architecture chapter of the Statewide technical architecture. Identification security for smart cards is based on:

- The user having physical possession of the smart card
- The user knowing the password or PIN to activate the card 's function
- The security functions available on the cards
- The tamper-resistant qualities of the card

The host software supports the attachment of the smart card reader to the host platform (e.g. workstation) and the identification functions required interacting with the smart card. Neither the reader nor the smart card trusts each other without a successful completion of the security process. A smart card together with a user password or PIN forms the basis of identification. The user must enter the correct password or PIN before the card will allow access to its resources. If the attempts to access the card exceed a user-specified number of attempts, the card will disable itself or even destroy itself and its contents if that is preferred. Like a password, the card can be re-enabled after failed attempts unless it has destroyed itself. Smart cards are designed to resist tampering and external access to information on or used by the card. The ultimate decision on whether to carry out the identification transaction is made by the card, strengthening the security of smart card-based identification. Smart card authentication is based on cryptography and is used in the authentication process. This authentication is based on both public key and secret key cryptography. Cryptography and authentication are discussed in the next section on authentication. A smart card used for identification can include a variety of useful security functions including:

- Storage of passwords for access to systems networks information stores, etc.
- Storage of public and private keys for authenticating identity.
- Storage of public and private keys for encrypting information to ensure privacy.
- Performing encryption for authenticating identity

Smart cards extend identification to something the user physically holds. They are, therefore, more effective than schemes based solely on something the user knows such as a password. In the future, biometrics will be used in conjunction with smart cards to ensure that unchangeable characteristics and security functionality can be combined in one technology.

6.3 Identification Security Best Practices

Best Practice 1: Use risk management techniques when considering Biometric Identification.

- Biometrics as an identification tool is relatively new and expensive.
- Biometrics techniques vary in success in real environments. Testing under actual conditions is necessary to determine effectiveness.
- Application integration with biometrics is hampered by a lack of standard APIs.

Best Practice 2: Make user-IDs unique within an agency.

- Each agency should adopt and use a consistent format within that agency.
- Agencies without an existing user-ID schema should consider consolidating all user-IDs under the State schema (**need to reference where this schema can be found here**).
- Each user should have an individual user-ID. Generic, multi-user-Ids should be avoided due to an inability to assign accountability.

Best Practice 3: Include user-ID policies in password policies.

- Password policies should be consistent with federal FIPS 112 standards.
- Passwords should not be shared.
- Passwords should have a minimum length, expiration date, reuse limitations, and revocation upon maximum number of invalid attempts.
- Password policies should be emphasized in security awareness programs.

Best Practice 4: Leverage existing technology infrastructure (i.e. ODN – Security Dynamics) when using proprietary tokens.

- Using a single token technology across the enterprise minimizes integration and implementation problems and avoids expensive compatibility issues.
- Proprietary tokens require strong management.
- Using a single token technology reduces cost and increases likelihood of successful implementation.

Best Practice 5: Use risk management techniques when considering smart cards.

- Smart cards require well-developed management procedures. The cost of the technology combined with the cost of managing smart cards dictates that they are used in situations where less expensive identification technologies are inadequate.
- Smart cards are most often used when there is a need to support multiple applications, or there is a need for additional storage capacity on the cards as opposed to tokens, and there is a need for a high level of security.

Best Practice 6: System Access

System access should be granted via a formal and audible process, and should be accompanied by security training that is commensurate to one's duties and responsibilities.

Best Practice 7: Non-disclosure Agreements
Non-Disclosure Agreements should be signed by all individuals who need access to "sensitive" information, prior to granting access to that information.

Best Practice 8: Background Checks
Background checks of personnel may be required to be consistent with Agency policy and depending on the sensitivity of information accessible to that position.

6.4 Identification Security Implementation Approach

Obsolescent and Transitional Technology	Current Strategic Technology	Emerging Technology
Proprietary APIs for identification	Industry standard and vendor neutral APIs for identification.	Human Authentication API (HA-API).
Proprietary tokens, which do not use leverage existing State infrastructure.	Security Dynamics ACE Server	

- When a proprietary standard becomes widely used it becomes a defacto standard, even if a standards committee did not develop it. RACF is an example of a defacto access control standard. Defacto standards should be considered "industry standard " and need not be avoided.
- Whenever possible, attempt to leverage existing State security infrastructure unless there is a specific requirement that makes this infeasible.
- Whenever possible, utilize technologies and products that can be used across agencies. Interoperability is highly desirable. Non-interoperable products should be avoided.

6.5 Identification Security Standards

Standard 1: Adopt current public safety standards for fingerprint identification.
Whatever fingerprinting standards are in place by the Arizona Department of Public Safety for State employees should be followed. This should also take into consideration any federal requirements such as IRS requirements for exchanging information with State tax departments.

Standard 2: ISO 7816 smart card standards for contact smart cards.
ISO 7816/1-4 standards define the electrical resistance, positioning of electrical contacts, communication protocol between card and card reader, and command set recognized by smart cards. These correspond roughly to the OSI layered model. The command set defined by the ISO 7816-4 standard are included in whole or in part by most smart cards on the market
.
Standard 3: ISO 14443A and Mifare smart card standards for contacts smart cards.
ISO 14443A standards for contacts smart cards define the characteristics and communication protocols between contacts cards and card reader. These standards are still in development. The Mifare architecture is the de facto global interface standard for contacts and is based on ISO 1443A. Contacts cards under this standard use RF power and frequency protocols and cover read/write distances up to 10cms of the reader.

Standard 4: Use PKCS #11 or PC/SC for integration of smart cards and host/reader-side applications.
PKCS #11 from RSA is a widely accepted standard for integrating smart cards to applications supported by many vendors. PC/SC is also widely accepted for integration of smart cards on wintel platforms. Use either PKCS #11 or PC/SC when integrating smart cards into applications.

Standard 5: Speaker Verification API (SVAPI).
SVAPI is an API used for incorporating speaker-recognition technology into desktop and network applications. A consortium of vendors, technology developers, researchers VARs and end-users developed the SVAPI. The SVAPI offers interoperability over distributed environments with related APIs. They include SAPI, the telecom industry 's S100, a standard architecture for developing computer-telephony applications, and Java Speech, a standard for speech recognition using Java.

Standard 6: Human Authentication API version 2.0 (HA-API).
The Human Authentication API (HA-API) is a generic API designed to allow a common set of instructions to integrate biometrics into applications requiring identification. It supports the enrollment sampling, processing and verification of biometrics. The API supports multiple biometric template types and multiple vendor technologies for each biometric type in one database. This permits an enterprise wide approach to biometric identification while allowing different application-specific biometrics to be used. A single database also facilitates the use of multiple biometrics in a single application. The API permits changing the biometric used without requiring application code changes. The HA-API specification was prepared for the US DOD by the National Registry, Inc. Currently the Open Group is considering adopting the HA- API as part of a common data security architecture. HA-API is defined for the Win-32 environment. Future versions will support other environments. The current HA-API only supports matching a user to a known template. Future releases will incorporate one-to-many identification. The HA-API is supported by a number of biometric vendors.

Standard 7: Granting Access to resources and information
The Owner must explicitly grant access to personnel. (i.e., not allowed by default)

Standard 8: Access Termination
Access must be terminated concurrent with when the requirement for access no longer exists. (e.g., as a result of transfer, termination, and changes of duties)

7.0 Authentication Services

Authentication X.509 Certificates PKI DCE/Kerberos

7.1 Introduction

Authentication is the process of verifying the identity of a user. Authentication answers the question: "Are you who you say you are?" It is the means of establishing and enforcing a user's rights and privileges to access specific resources. This in turn becomes the basis for individual accountability. There are three ways of authenticating a user's identity, which can be used alone or in combination: 1) validating something the user knows; 2) validating something the user possesses, referred to as a "token"; 3) validating something the user is, referred to as a "biometric". The most common method used to authenticate a user is a password. A password is a secret series of characters associated with an individual user-ID. A sign-on process to authenticate the user accepts a password and a user-ID. The sign-on process matches the password given with a stored password for that user-ID. If they match, the system has verified the user's identity. Passwords are inexpensive and widely integrated into today 's systems.

Passwords have various weaknesses. User passwords are often poorly chosen, lack adequate administration, and present a danger of passwords being intercepted and read over unsecured communication links. Electronic business transactions have stricter requirements on uniquely identifying and authenticating the sender or recipient of electronic information. These can be satisfied with a 'digital signature,' which is the electronic equivalent of a handwritten signature. Authentication techniques such as Public Key Certificates have been developed to address the strict authentication requirements of electronic business processes. This technology is based on cryptography, which is introduced here, and discussed further in Section 8.0 - Authorization and Access Control Services.

Once authenticated, logical access controls are utilized to authorize and enforce a user's access to and actions towards specified resources. This authorization may be based on identity, roles, location, time, types of transactions, service constraints, access mode, or a combination of these criteria. Both internal authorization safeguards and external controls can be deployed.

7.2 Authentication Security Technology Components

The technology components used in authentication are based on existing and emerging standards. Implementation differences, even where standards are used, can raise barriers to enterprise-wide solutions. For an enterprise-wide security infrastructure to succeed, the technologies must use open interoperable protocols and standards. While complete solutions do not exist, the basic components are currently available. The technology components used in authentication are:

Cryptography:
Cryptography is a technology used to protect the confidentiality of information. It forms the basis for ensuring the integrity of information and authentication of users. Cryptography uses algorithms to scramble (encrypt) and unscramble (decrypt) information such that only the holder of a cryptographic 'key ' can encrypt or decrypt the information. A cryptographic 'key ' is a string of alphanumeric characters used along with the information as input into a cryptographic algorithm.

Public Key / Private Key Technology:
Authentication which requires the unique identification of a user is often based on Public /Private Key cryptography. This form of cryptography uses two related keys. Information encrypted with one key can only be decrypted with the other key. The 'Public' Key is made openly available in a repository to anyone who wants to communicate with the user in a secure manner. The 'Private' Key is kept only by the owner and is never divulged. Since only the Owner has the private key, its use is considered sufficient to uniquely authenticate the owner. A digital signature is an example of a private key being used to verify that the sender (originator of the information) is really who they say they are. One potential use of public key/private key is a taxpayer using their private key to authenticate themselves to a tax department. The tax department recovers the taxpayer 's information by using the taxpayer's public key. Since only the taxpayer's public key can recover what was encrypted with the taxpayer's private key, the tax department is assured it came from this particular taxpayer.

Public Key Certificate:
A user's public key is distributed using an electronic document called Public Key Certificate. This certificate contains the user's name, public key, an expiration date and other information. It is considered reliable when a trusted authority digitally signs it. Trusted authorities that issue Certificates are known as Certificate Authorities and are covered in a later section.

Message Digest:
Message digests are used to ensure the integrity of information. Integrity means that information cannot be altered without detection. Information is put through a mathematical 'hash' function. This function reduces the information to a small numeric value called a message digest. Even the slightest change to the information would generate a different message digest. To verify information has not been modified, a user applies the same hash function on the suspected information to generate a message digest. If the resulting message digest matches the original message digest, the information has not been changed. One important use of message digests is in digital signatures.

Digital Signature:
Digital signatures are the equivalent of a handwritten signature in that they tie an individual to a document. The first step in digitally signing an electronic document is to generate a message digest of the document. The signer encrypts this message digest using the signer's unique private key. The document and encrypted message digest are sent to one or more recipients. Verifying a digital signature is the reverse process. The recipient generates a message digest from the document. By using the signer's public key, the recipient can recover the original message digest from the encrypted one. This proves it must have come from the signer since only they have the private key. If the recovered and the generated message digests are equal, the document has not been modified and the sender cannot deny their digital signature. The digital signature, therefore, provides non-repudiation, which means that the sender cannot falsely deny having sent the message.

Public Key Infrastructure (PKI):
The Public Key Infrastructure (PKI) performs the generation, distribution and management of public keys. A Public Key infrastructure incorporates Certificate Authorities and related functions, which are discussed in a later section. A PKI includes the following services:

- Certificate generation, distribution, update, and revocation.
- Key histories, backup and recovery.
- Certificate repositories.

PKI is an emerging technology that is largely untested in large-scale deployments. It will be necessary to incorporate PKI technology into some electronic business applications and to lay a foundation for more extensive use in enterprise-wide security. The transition to enterprise-wide integration will include using certificates for authentication in some applications, alternative means of authenticating users in other applications, and secure communications elsewhere when necessary.

7.3 Authentication Security Best Practices

Best Practice 1: Authenticate users prior to accessing private system resources or services.

- In some instances anonymous access to systems is necessary and desirable (e.g. public web servers). However, when accessing private systems, users should always be authenticated prior to granting access.
- Authenticating users is the basis for providing accountability.

Best Practice 2: Use Public Key Infrastructure for authentication when digital signatures are required.

- Digital signatures are required for many types of electronic business.
- Using PKI when digital signatures are required will promote interoperability between agencies.

Best Practice 3: Use an enterprise-wide Public Key Infrastructure (when available).

- A unified approach to a Public Key Infrastructure enables the State to respond to changing requirements and conditions.
- A fragmented approach to Public Key Infrastructure will complicate administration and management of security across the enterprise.

Best Practice 4: Use token-based or strong password-based authentication where public key certificates are not feasible and a high degree of security is required.

- Token-based systems offer a higher level of security than passwords.
- Where token-based identification is not possible, a password policy based on best practices can provide an acceptable level of security.

7.4 Authentication Security Implementation Approach

Implementation Guideline 1: Make use of strong password controls for all legacy applications.

All legacy applications must implement strong password controls consistent with password best practices.

- Strong password usage is a minimal requirement for authentication.
- Proper password policy and usage should be emphasized in all security awareness programs.

Implementation Guideline 2: Avoid use of proprietary certificate extensions to ensure later interoperability.

7.5 Authentication Security Standards

Standard 1: Public Key Certificates (X.509v3)
Public Key authentication must be based on Public Key Certificates. Certificates must be based on the X.509v3 standard. Despite the widespread acceptance of this standard, care must be taken when dealing with vendors. Projects should require proof of interoperability with existing or proposed enterprise implementations using X.509v3 certificates. Proprietary extensions to certificates could inhibit interoperability and should be avoided.

Standard 2: Ownership
Each Agency must ensure that authentication, authorization and data security, as established by the data owner, is not compromised during data sharing and systems interoperability.

Standard 3: Authentication Control
Each Agency must establish a formal authentication control policy that establishes the criteria for administering authentication safeguards, (e.g., a formal password policy that includes the criteria for password aging, history, length and composition)

Standard 4: Storing Sensitive Data
Each Agency must store all sensitive data used in authenticating the user, including passwords, in protected files.

Standard 5: Least Privilege
Each Agency must authorize based on least privilege. Least privilege states that a user is given only that set of privileges necessary to perform his/her job.

Standard 6: Use of Cryptology Technologies
The use of cryptology technologies for data storage and data communication (transmission of data) must be based on open standards.

8.0 Authorization and Access Control Services

8.1 Introduction and Background

Authorization answers the question: "Are you allowed to do what you are attempting to do?" Requirements for use, and prohibitions against use, of resources vary widely across the enterprise. Some information may be accessible by all users, some may be accessible by several groups or departments, and some may only be accessible by a few individuals. Access to applications, the data they process, and database modifications must be carefully controlled. Authorization is the permission to use a computer resource. Access is the ability to do something with a computer resource. Access controls are the technical means to enforce permissions. They allow control over what information a user can use, the applications they can run and the modifications they can make. Access controls may be built into the operating system, may be incorporated into application programs or major utilities, or they may be implemented in add-on security packages. Access controls may also be present in devices that control communications between computers (e.g. routers).

Access controls help protect:

- Operating systems and other system software from unauthorized modification, thereby helping to ensure system integrity and availability.
- The integrity and availability of information by restricting the number of users and processes with access to the information.
- Confidential information from being disclosed to unauthorized individuals.

Internal Access Control
Internal access control protects information that is being accessed from within the agency or enterprise network. Internal access control is applied at points in the information infrastructure where potential damage may occur. Internal authorization and access control should be implemented:

- At the platform
- To stored information
- To information in transit
- For distributed applications

Platform Access Control
Platform access control will be addressed through the combined efforts of the Platform and Security Component Committees. Platform access control will be addressed by a future release of this document.

Stored Information Access Control
Stored information access control will be addressed through the combined efforts of the Information and Security Component Committees. Stored Information access control will be addressed by a future release of this document.

Distributed Applications Access Control
Distributed applications access control will be addressed through the combined efforts of the Applications, Systems Management, and Security Component Committees. Distributed applications access control will be addressed by a future release of this document.

Information in Transit Access Control
Information in transit access control is the means to prevent unauthorized access to data and information transported across networks. A multi-platform, interoperable set of access control services has yet to be fully specified in industry. The choice of security approach depends on application capability and requirements, advantages of a particular approach, architecture support for a particular choice, and enterprise-wide decisions on securing communications. Securing data over networks can be accomplished in various ways:

- Within applications using available security mechanisms
- Between applications on encrypted links
- At lower layers of a communication protocol to secure communications across a network

External Access Control
External access controls are a means of controlling interactions between enterprise resources and outside people, systems, and services. External access control should permit authorized remote access by employees of the enterprise, citizens, and external trading partners. External access control must also ensure that confidential information transported outside the enterprise is protected from unauthorized access. External access controls use a wide variety of methods, including physical devices.

Protecting the enterprise from unauthorized external access can be accomplished by:

- Perimeter defenses such as firewalls
- Remote access control at the perimeter
- Secure communications from the enterprise to external authorized parties
- Layered defenses at points and components of infrastructure within the firewalls

Data Security
Data Security refers to those practices, technologies and/or services used to ensure that security safeguards are applied appropriately to data that is provided, processed, exchanged and/or stored by the State. Data security safeguards strive to sustain the level of integrity, availability and confidentiality of this data as stated by the Agency's policy. Data security is the responsibility of the data owner. The appropriate types/pieces of data and their level of sensitivity should be identified as part of the business impact analysis and risk assessment activities.

Examples of data security safeguards include Agency developed procedures, vendor delivered configurable controls (e.g., automatic screen savers), and add-on technologies (e.g., hashing algorithms). Data security safeguards are clearly interdependent with other safeguards described with this architecture.

8.2 Access Control Security Technology Components

The technology components used in authorization and access control are based on existing and emerging standards. Implementation differences in these technology components can raise barriers to enterprise-wide solutions. Technology components for protecting operating system and system software, enterprise data and networks from unauthorized access will be covered in a later release of this section. The technology used to protect the enterprise from unauthorized internal and external access and ensure the integrity and confidentiality of information used by the enterprise includes:

Cryptography:
Documents, communications, and data travel inside and outside the enterprise in electronic form. Electronic information is easy to read, modify or replace without detection. However, in many situations, the confidentiality of the information in transit must be maintained, e.g., taxpayer data, credit card and bank account numbers, and child abuse cases. Information transported across the State's TCP/IP networks and across the public Internet is passed in clear text. Malicious individuals can intercept, view and modify this information using easily obtained tools. As described in the authentication section above, cryptography is a means to scramble information such that only authorized entities (people or processes) have access to the information. A combination of public key cryptography and secret key cryptography can be used to implement authenticated and protected communication for secure access control. Most bulk encryption of information involves the use of secret key cryptography.

Secret Key Cryptography:
Secret key technology is a form of cryptography where encryption and decryption use the same key, a 'secret' key. Pairs of users or processes share the same secret key. Data encrypted with a secret key is decrypted using the same secret key. Secret key technology is used to do most encryption because it is much faster than other techniques. Examples of commonly used secret key algorithms include DES, 3-DES, RC2, RC4, IDEA and CAST.

Cryptographic Algorithms (The terms "Obsolescent, Transitional, Strategic, and Emerging" are defined in the Glossary in Appendix C.)

Obsolescent	Transitional	Strategic	Emerging
Public Key: Rivest-Chor Merkle-Hellman	**Public Key:** Rabin Diffie-Hellman ElGamal LUC (Lucas seq)	**Public Key:** RSA (Rivest-Shamir-Adleman) DSS (Digital Signature Standard) ECC (Elliptic Curve)	**Public Key:** XTR (Efficient Compact Subgroup Trace Representation) NTRU
Secret Key: RC2	**Secret Key:** OTP (One Time Pad) DES (Digital Encryption Standard) RC4	**Secret Key:** 3DES (Triple Digital Encryption Standard) IDEA (International Data Encryption Algorithm) Blowfish	**Secret Key:** AES (Advanced Encryption Standard) Twofish MARS RC6 Serpent
Hash Functions: MD2 (Message Digest 2) MD4 (Message Digest 4)	**Hash Functions:** MD5 (Message Digest 5)	**Hash Functions:** SHA-1 (Secure Hash Algorithm)	**Hash Functions:** RIPEMD-160 (Race Integrity Primitives Evaluation Message Digest)

Security Protocols:
Protocols are well-defined message formats used for communicating in networked systems. The lack of a set of widely inter-operable standards raises barriers to enterprise-wide solutions. When considering products, it is useful to check present and future planned compliance to standards. Important security protocols are described below:

- **Secure Sockets Layer** –(SSL) is a widely used means for securely communicating between a Web browser and Web server. SSL creates an encrypted link between a client and server that need to communicate securely. Both client and server authentication is possible. SSL can also be used with other applications such as ftp, telnet, etc.
- **Simple Key Management for Internet Protocols** –(SKIP) is a secret key exchange protocol that operates below the IP layer in a TCP/IP communications protocol. This method can be used to provide transparent security between entities.
- **Security Multi-parts for MIME** (S/MIME) is an application security protocol. It is implemented for email but has wider implications for store-and-forward messaging.
- **Internet Protocol Security Extensions** (IPsec) is a security protocol defined for IP networks, which operates at the network layer in TCP/IP communications protocol. IPsec adds header extensions to the IP communications protocol and is designed to provide end-to-end security for packets traveling over the Internet. IPsec defines two forms: sender authentication and integrity, but not confidentiality, through the use of an Authenticating Header (AH), and sender authentication, integrity and confidentiality through the use of an Encapsulating Payload (ESP).
- **Internet Key Exchange** (IKE) provides secure management and exchange of cryptographic keys between distant devices. It is the standard key exchange mechanism for IPsec.

Firewalls:
Firewalls are a common term for physical devices, software and network architectures designed to block or filter access between a private network and a public network such as the Internet. They can also be used to provide access control between separate internal networks. Firewalls enforce the enterprise's security policy at determined perimeters, e.g., access point to the public Internet. To be effective, each must provide the single point of access to and from an untrusted network. Firewall technology is rapidly evolving. There are two basic types of firewalls, Packet Filtering and Application Gateways (proxy servers). The network architecture and location of firewalls relative to internal networks is an important consideration in securing internal networks. Packet Filtering firewalls filter access at the packet level. By examining the contents of packets, they permit or deny access based on a defined access control policy. Packet filtering firewalls operate below the application and typically do not have access to information particular to an application. Application level firewalls or proxy servers protect internal networks by not permitting direct access from the internal network to untrusted networks such as the public Internet. Internal users connect to the 'proxy' which then acts on their behalf, completing the connection to the requested external service. Proxy firewalls are specific to the applications they proxy. For example, a proxy for Web or FTP is installed to support those applications. Not all applications can be proxied. For those that can 't be proxied, proxy-like gateways shuttle data between internal and external networks. They maintain the characteristic of preventing direct connections between the internal and external networks. The network architecture used in deploying firewalls can provide additional protection. By placing a sub-network between the internal network behind the firewall and the external public Internet, multiple security breaches would be required to penetrate the internal network. This additional sub-network is referred to as a 'Demilitarized Zone ' (DMZ). Multiple DMZs can be employed to protect sub-networks within the enterprise.

Virtual Private Networks (VPNs):
Virtual private networks are ways of connecting two networks over insecure networks such as the public Internet. A VPN establishes a secure link by using a version of the IPsec security protocol. These links are typically implemented between firewalls. VPNs today often use proprietary record structures and have inter-operability problems. A secure communications link between the networks does not ensure that communications beyond that link are secure. Some VPNs use a variety of non-IPsec protocols. These include PPTP, L2TP and L2F and proprietary protocols. These protocols offer similar services but are better suited to remote-access applications and non-IP traffic across the public Internet. These protocols have their uses but are not covered in this document.

8.3 Access Control Security Best Practices

Best Practice 1: Authorize users based on least privilege.
Authorize users to the minimum set of resources required for their role.
- Authorizing users on least privilege minimizes the impact of security violations.
- Authorizing users to a minimum set of resources required to their function makes it easier to establish accountability.

Best Practice 2: Define appropriate security levels and use these levels for each segment of the infrastructure to minimize security management in response to changes.
Use appropriate security levels for each part of the information infrastructure.
- Different parts of the information architecture will require different security levels.
- A basic level of communication security will reduce the number of applications that must be security-aware.

Best Practice 3: Use open standards-based security solutions.
Using open standards-based solutions will facilitate inter-agency communications and data exchange.
- Use of proprietary solutions will make it difficult to adapt to advances in security and standards development.
- Use of proprietary solutions will make inter-agency communication more difficult.

Best Practice 4: Involve security team in the process of selecting protocols.
The security team can assist with selecting open standards-based protocols that place security in the appropriate location in the architecture.

8.4 Access Control Security Implementation Approach

Obsolescent and Transitional Technology	Current Strategic Technology	Emerging Technology
Proprietary security products.	Open standards-based security using SSL, IPSec, S/MIME.	Content filtering.
Open non-Firewalled Web, FTP, Mail, DNS servers	Firewalled, with services placed on DMZ.	
Critical or Confidential data transmitted in clear text.	S/MIME for email, SSL and IPSec for confidential internal and external data in transit.	
Open remote access to the enterprise	Strictly controlled remote access to the enterprise (RADIUS, TACACS).	

Implementation Guideline 1: Secure transmission of data where appropriate.
Information in transit must be secured where appropriate.

- Data in transit to and from the enterprise must be protected in compliance with legal requirements for confidentiality and privacy.
- Web-enabled applications must protect confidential or critical data from unauthorized access.
- Use secure server-to-server communication to protect confidential or critical data transmission.

Implementation Guideline 2: Avoid Virtual Private Network (VPN) solutions for connecting trading partners outside the enterprise that are not IPsec compliant.
Avoid use of VPN solutions that are not IPsec compliant to connect to outside trading partners.

- Most VPN solutions today are proprietary. All outside trading partners are unlikely to use the same or similar technology.
- VPN solutions should be chosen based upon IPsec compliance and inter-operability among IPsec compliant VPNs.

Implementation Guideline 3: Use SSLv3 client authentication where required for web-enabled applications when appropriate.
Web-enabled applications that require user authentication should use SSLv3 with client authentication and client public key certificates where appropriate.

- SSLv3 without client authentication is sufficient protection for certain types of transactions, for example, credit card purchases over the web.
- SSLv3 with client authentication should be used applications that mandate user authentication.

Implementation Guideline 4: Use encryption for stored data or email only when appropriate.

- Encryption and decryption of stored data incurs a high overhead. It should be used only where appropriate.
- Managing encrypted data requires effective key recovery and escrow procedures.

8.5 Access Control Security Standards

Standard 1: Secure Sockets Layer version 3 (SSLv3)
SSLv3 is the most commonly supported protocol for communication between web server and browser. It authenticates the web server and optionally authenticates the user browser. Current implementations allow for client authentication support using the services provided by Certificate Authorities.

Standard 2: IP Protocol Security Extension (IPsec)
IPsec is an extension to the IP communications protocol, designed to provide end-to-end confidentiality for packets traveling over the Internet. IPsec works with both the current version of IPv4 and the new IPv6 protocol. IPsec has two modes: sender authentication and integrity but not confidentiality through the use of an Authenticating Header (AH), and sender authentication and integrity with confidentiality through the use of an Encapsulating Payload (ESP).

Standard 3: Cryptography must be based on open standards. 56-bit encryption is the minimum acceptable standard. 40-bit encryption is unacceptable and 128-bit is desirable.
Cryptographic services identified in this document are based on open industry accepted standards. The following business requirements and associated cryptographic standards have received wide acceptability. Only full strength cryptography should be used. For example, browsers are often supplied with weakened versions such as 40 bit DES, RC2 and RC4. Only browsers with full strength keys should be used for transactions involving the State. Cryptography with variable length keys should use a minimum key length equivalent to 56 bit DES.

Cryptography Algorithm	Standards
Public Key /Private Key	RSA (1024 bit keys), ECC (160 bit keys)
Secret Key	DES, 3-DES, RC2, RC4, I DEA, CAST (minimum DES equivalent or full length keys)
Message Digest	MD5,SHA-1

Standard 4: Use S/MIME version 3 for securing email communications.
S/MIMEv3 provides a consistent way to send and receive secure email including MIME data. S/MIME defines a protocol for encryption services and digital signatures. Email clients should be evaluated for support of the standard and for inter-operability.

Standard 5: Place Internet application and access services on the DMZ or proxied from the DMZ.
Services provided through the Internet must be placed on or proxied from the DMZ

- Application services must be protected from unwanted external access and must be placed on the DMZ or proxied from the DMZ.
- Communication from servers on the DMZ to internal applications and service must be controlled.
- Remote or dial-in access to the enterprise must be authenticated at the firewall or through authentication services placed on the DMZ.

9.0 Security Administration

9.1 Introduction and Background

All organizations experience change. Keeping security systems synchronized with organization changes is essential. Employee additions, transfers, and resignations must result in corresponding security changes rapidly. The complexity of administering security in a distributed environment can be reduced by:

- Creating an organization structure that includes well-defined security responsibilities.
- Simplifying the complexity of administering security while meeting defined security requirements (e.g., role-based administration instead of user-based administration).
- Creating security domains with common security requirements and policies.
- Leveraging tools for performing administrative functions.

9.2 Administration Technology Components

Security Domains
Security domains are areas within the enterprise, which adhere to a specific security policy and its enforcement. These could be administrative domains (such as departments) or resource-based domains (computing environments), or even geographic domains. Security domains can even overlap. The enterprise, as a whole, can be considered one security domain and policies can be applied at entry points to the domain. Within the enterprise domain may be multiple security domains, which are defined administratively. These sub-domains may have different security policies. Security domains are identified and maintained at their boundaries. The enterprise security domain is protected by Firewalls, which implement security policy at the perimeters of the enterprise. Security domains within the enterprise can be defined in a similar manner.

Certificate Authority (CA)
Public Key Certificates are used to authenticate users and establish non-repudiation of sender or recipients of information. A Certificate Authority (CA) performs the management of certificates in a Public Key Infrastructure. While a Public Key Certificate connects a Public Key to a person or entity, there may be an additional concern that the certificate is not valid (i.e. someone may be masquerading as the person). This has raised the requirement for a 'trusted third party' that can issue certificates in a manner acceptable to all. This trusted third party is known as a Certificate Authority (CA). CAs are a necessary component of Electronic Business. A CA is both a physical entity, to ensure a physically secured environment for the required systems, and a software system that actually performs the operations required to issue, verify and revoke certificates. Certificate Authorities are usually centralized and hierarchical. A typical centralized implementation would be to have a CA for the enterprise, one or more CAs at a regional or state level and so on. Since individuals requiring certificates are local, the function of verifying the validity of a certificate request is often localized. This local function is referred to as a Registration Authority (RA). In the process of issuing Public Key Certificates, the Registration Authority is responsible for verifying the identity of the requestor and communicating that to the CA. Different methods may be used to verify a requestor, including visual identification. RAs may be at a department or agency level. Their close proximity to the users allows them to take responsibility for revoking certificates when a user leaves employment or a Private Key is compromised.

Systems Interoperability Security

Systems interoperability refers to those practices, technologies and/or services used to ensure that security safeguards are applied consistently and appropriately to mechanisms that allow diverse systems and networks to interoperate. Agencies often depend on interoperability for the timely exchange and sharing of information and data to effectively perform their business services. An Agency's systems may interoperate with those of other Agencies, other governmental bodies (local, state, or federal), with businesses or with public users; and those systems may operate on different platforms or with different technologies. Synergies, cost savings, and economies of scale can result by ensuring that security safeguards between "interoperating entities" are compatible and sustain the desired security protection levels of those entities. Industry best practices suggest that deploying vendor-neutral, open standards provides a common denominator in support of interoperability. The table below provides guidance regarding widely accepted industry security protocols.

Security Protocol for:	Obsolescent	Transitional	Strategic	Emerging
WWW connections			SSL/TLS (Secure Socket Layer/Transport Layer Security)	SHTTP (Secure Hypertext Transfer Protocol)
E-mail Security			Open PGP (Pretty Good Privacy) Secure MIME (Multi-purpose Internal Mail Extension)	
Terminal sessions & TCP connections.		SSH1 (Secure Shell)	SSH2 (Secure Shell)	
Distributed Name Services				DNSSEC (Domain Name Server Security)
API to cryptographic algorithms				GSSAPI (Generic Security Services API)
Network Tunneling		PPTP (Point to Point Tunneling)	IPSec (Internet Protocol Security) L2TP (Layer Two Tunneling Protocol)	
Key Exchange			SKIP (Simple Key Management for Internet Protocol)	ISAKMP (Internet Security Association Key Management Protocol)

Sign-on Administration
Sign-on administration will be developed and included in a later release of this section.

Key Recovery/Escrow
Information that is encrypted must be able to be recovered should the original encryption 's keys no longer be available. A key recovery or key escrow mechanism should be in place. Keys may need to be escrowed for future verification of digital signatures. (Key recovery will be addressed in a later update).

Incident Handling
Incident handling refers to those practices, technologies and/or services used to respond to suspected or known breaches to security safeguards.

Once a suspected intrusion activity has been qualified as a security breach, it is imperative that the incident be contained as soon as possible, and then eradicated so that any damage and risk exposure to the Agency and the State are avoided or minimized. Information technology security incidents refer to deliberate, malicious acts, which may be technical or non-technical. In several cases, if the incidents are left unchecked, then the damage resulting from these incidents continues to spread within, and across, Agencies.

Handling incidents can be logically complex, and may require information and assistance from sources outside the Agency, law enforcement entities such as technical specialists, DPS or the FBI, and the public affairs office. Industry best practices suggest that organizations that adopt both proactive and reactive means to address incident handling are better able to limit the negative implications of incidents.

Security Awareness
Security Awareness refers to those practices, technologies and/or services used to promote User awareness, User training and User responsibility with regards to security risks, vulnerabilities, methods, and procedures related to information technology resources. A "User" is defined as an individual or group who has access to an information system and./or its data.

Users within an Agency need to understand the sensitivity of the Agency's information resources and their responsibility in protecting those resources. For example, Users should be aware of the threats and the associated impacts of a compromised password; of potential viruses transmitted over the Internet; of corrupted databases; and of the accessibility of printed information generated from the system.

Although responsibility to adhere to State statutes and Agency policy and procedures are accepted by personnel upon engagement, Security Awareness programs provide a proactive mechanism to foster further comprehension of an individual's security responsibilities:

- to contextualize security responsibilities to specific job duties and case examples
- to motivate personnel towards a security-conscious behavior while performing their duties
- to reinforce the consequences of security failures on the State, the Agency, its mission, its customers, and the User.

The appropriate amount, depth, and timing of Security Awareness is a risk-based decision. Best practices suggest that a Security Awareness program that utilizes a combination of periodic training sessions (introductory/refresher) and on-going security awareness promotion (marketing) are most effective. In addition, where appropriate, an Agency may decide not to grant certain access rights to personnel until the desired level of Security Awareness Training

has been successfully completed. Lastly, as the business and technical environment changes, security awareness material will need to be updated accordingly.

9.3 Security Administration Best Practices:

Best Practice 1: Employ a security model that simplifies administration and maintenance.

- Effective administration is required to implement a secure information infrastructure.
- Security systems that are difficult to set up and maintain are more likely to ultimately fail.
- Other best practices listed here help simplify administration and maintenance (e.g. role-based administration, standards, documented processes and procedures, automation, training, documented roles and responsibilities, etc.).

Best Practice 2: Use a role-based administration model.

- Role-based administration is the practice of assigning rights and permissions to directory objects which represent a particular role (e.g. group objects in NT or NetWare, Organization role objects in NetWare, etc.) rather than assigning rights to an individual user object. For example, certain members of an IT staff may need access to an Asset Management system for tracking leased equipment. In this case, a group should be created and the rights needed to run the application assigned to that group.
- Role-based administration reduces complexity and the amount of effort needed to administer information infrastructure security.
- Permissions and rights should not be directly assigned to a user object with the exception of home directories. All user permissions or rights should stem from group or role membership(s).

Best Practice 3: Develop, document, and promote platform-specific standards, best practices, processes, and procedures (e.g. naming standards, addressing standards, procedures to change a user's last name, etc.).

- Improves manageability while lowering administrative costs.
- Reduces "learning curve " for new systems administrators and promotes consistency.

Best Practice 4: Obtain automated administrative tools to reduce complexity.

- Automation of recurring administrative tasks reduces the amount of time needed to respond to organizational changes.
- Automation promotes consistency and improves manageability.
- Improves administrator productivity and reduces errors.

Best Practice 5: Plan for security when developing applications.

- Leverage existing application, system, or platform security mechanisms where possible. Develop application-specific security mechanisms only where necessary.
- Separating security functions from the application enables the developer to focus on meeting application requirements.

Best Practice 6: Create an organizational structure with defined and documented security roles and responsibilities.

- Well-defined roles and responsibilities provide accountability for security tasks.
- Defined roles and responsibilities simplify administrator and user security training.
- Include non-IT resources and their roles and responsibilities (e.g. Human Resources has to provide information on employee changes).

Best Practice 7: Provide a strong training program for systems administrators.

- Training investment helps reduce administrative costs, improve productivity, and reduces errors.
- Training costs can be controlled and effectiveness improved when combined with automation, documented system standards, processes, and procedures.

9.4 Security Administration Implementation Approach

Obsolescent and Transitional Technology	Current Strategic Technology	Emerging Technology
User-based administration	Role-based administration.	N/A
Sign-ons that work only for a single platform or application.	Standards-based platform sign-ons. Domain authentication. Applicable across platforms.	Single sign-on.

9.5 Security Administration Standards

Standard 1: Incident Response Plans
Each Agency must develop an Incident Response Plan, which identifies the responsibilities and actions to be taken in response to incidents.

Standard 2: Statewide Information Protection Center (SIPC) Reporting
The State's Information Protection Center is responsible for providing a communication vehicles(s) and establishing service(s) in support of Agency incident handling and reporting.

Standard 3: Out-of-band Alternatives
Each Agency must ensure that out-of-band alternatives are established as part of their Incident Response Plan (i.e.; that the "compromised" device, platform, or media is not used to notify users or to report the incident to the SIPC.

Standard 4: Security Awareness Program
Each Agency must establish and maintain information technology security awareness programs to ensure that all individuals are aware of their security responsibilities and know how to fulfill them.

There are currently no industry-accepted standards for administering distributed systems. The systems management committee will cover standards used to help manage components of the information infrastructure (e.g. SNMP, RMON, etc.).

10.0 Security Audit

Audit Audit Tools Monitor / Filter Network Integrity Intrusion Detection Virus Protection

10.1 Introduction and Background

Audit is the process of monitoring the identification, authentication, authorization and access control, and administration of information infrastructure security to determine if proper security has been established and maintained. The security architecture must provide the capability to track and monitor successful and unsuccessful interactions with the information infrastructure. Accountability for interactions must be tied to specific users. The architecture should be able to audit all security services including identification, authentication, and administration.

Auditing systems activities provides a means to access policy compliance, verify operational assurance, maintain individual accountability, and support intrusion detection analysis programs. The actual process can be self administered within an Agency or independently administered externally. Personnel involved in these activities must have a high-level of expertise in the information technology security field and of auditing practices, and must administer said activities objectively.

Industry practices suggest that security safeguards tend to degrade over the operational lifecycle of systems as users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Agencies must therefore make a risk-based decision regarding the timing and scope of auditing system activities.

10.2 Security Audit Technology Components

The technology components and terminology for Audit services are discussed below:

Audit Security Tools
This section refers to those practices, technologies and/or services used to manage, analyze, filter, test and/or control security safeguards. For example firewall technology provides a mechanism through which authentication, authorization, filtering and directing or remote users to an internal system can be accomplished. Typically an Agency's security tool kit will be comprised of a combination of commercial off-the-shelf products, industry proven free shareware, and Agency developed software tools. The tools may be positioned on the perimeter of systems or layered and integrated into the systems, and may be deployed on either an operational or as needed basis. Specific examples may include firewall technologies, vulnerability scanners, and sniffers.

Monitoring & Filtering
Monitoring & Filtering technology will be developed and published in a later release of this section.

Intrusion and Threat Detection
Intrusion or threat detection refers to those practices, technologies and/or services used to: 1) detect that a suspicious activity may be occurring on systems/networks; and 2) to alert security administrators and security staff accordingly.

An attack on a system or network can come from either inside or outside the Agency. It could be intentional, (e.g., transmittal of viruses, "worms", or "Trojan horses") or unintentional (e.g., accidental deletion of a control file). Threat detection may include the real-time monitoring of activities such as logons, connectivity, operating system calls, command parameters, or system performance logs. Threat detection safeguards support the analysis of performance thresholds, behavioral anomalies, use patterns and trends (such as degradation in system performance over time), or the existence of known threats.

Threat detection may also include a review of activities 'after the fact', and over a specific time frame.

Alerts from automated threat detection tools may be active (immediate paging of appropriate security personnel) or passive (logging specific types of activities to a daily system security log for later review).

Virus Protection
Virus Protection technology will be developed and published in a later release of this section.

10.3 Security Audit Best Practices

Best Practice 1: Audit security processes as well as security events (authentication, access, attempted access, etc.).
- Defects in processes and procedures are security risks.
- Regular internal and external audits should include auditing security practices, policies, and procedures.

Best Practice 2: Audit security policies as well as processes and events.
- Policies are a security risk.
- Regular internal and external audits should include auditing security policies.

Best Practice 3: Use risk management techniques to determine which systems and resources should be monitored.
Auditing incurs significant costs in terms of system and human resources. Risk management techniques can ensure that these resources are maximized.

Best Practice 4: Agencies should have defined, documented, and tested procedures for responding to attacks (e.g. unauthorized access, denial of service, virus infections, etc.).
- Systems management tools can notify administrators of attack, but procedures are needed to ensure the desired response.
- Procedures should be thoroughly tested and documented.
- Procedures need to be linked with administrator and user communication and training.

Best Practice 5: Firewall technologies
Within the Agency, firewall technologies should be implemented to protect sensitive internal information and infrastructure.

Best Practice 6: Traffic Monitoring
Each Agency should have the ability to monitor and capture traffic at any location within their network.

Best Practice 7: Use of Sniffers and Scanners
Each Agency should use network and host vulnerability scanners to test for the vulnerabilities of internal systems and of perimeter defenses, and their adherence to security policy. Resulting vulnerabilities should be addressed.

Best Practice 8: E-mail Monitoring
Each Agency should scan all incoming e-mail for existence of malicious code and contain and eradicate the code.

Best Practice 9: Threat Alerts
Systems should be designed to handle both passive and active alarms

Best Practice 10: Security Event Logs
A security event log should be kept for each device. These logs should be analyzed, correlated and evaluated to identify and respond to suspicious activity.

Best Practice 11: Intrusion Detection Systems
Intrusion Detection Systems should be deployed both externally and internally to the firewall technology protecting the network.

Best Practice 12: CIMT Support
Agencies should get assistance from the Computer Incident Management Team provided by the State's Security Center as needed to trouble shoot unusual or difficult to isolate threats.

Best Practice 13: Notification of Threat
Violations of those parameters set in conjunction with the Agency's threat detection program should trigger an appropriate form of security notification to security administrators or security staff.

Best Practice 14: Configuration Management
System configurations and software change over time. Therefore, each Agency should audit security devices on a periodic basis to determine if compliance to security policies is being met.

Best Practice 15: Periodic Audits
Each Agency should have a security audit performed by a qualified and approved auditing party external to that Agency on an annual basis to supplement internal auditing activities.

10.4 Security Audit Implementation Approach

Obsolescent and Transitional Technology	Current Strategic Technology	Emerging Technology
Hardware and software with limited or no monitoring capability.	DMI, SNMP, RMON, etc.	
Third party tools that are extremely narrow or limited in scope (unless specific business requirements for the tool can be demonstrated). Single system or platform tools.	Automated notification based on thresholds.	Integrated tools with broad scopes.
Monitoring/Filtering tools with limited management capabilities.	Firewalls, host-based virus protection,	Perimeter virus protection.
Limited intrusion detection tools that lack extensibility.	Port scanners, sophisticated scanners (e.g. SATAN), Trojan-scanners.	Integrated, multi-platform tool sets.

Implementation Guideline 1: Define user roles, responsibilities, and frequency thresholds as baselines for audit and intrusion detection tools.

- Maximizes the investment in tools.
- Helps identify training needs.
- Ensures accountability.

Implementation Guideline 2: Virus protection systems should facilitate frequent signature updates and provide the ability to control or lock-down settings that could render the protection ineffective.

- Emergency virus signature updates in response to a rapidly spreading virus attack (e.g. Melissa) are becoming more common. Virus protection systems should allow for easy, fast updates to virus signatures on all systems where virus protection is used.
- Users should be prevented from disabling virus protection or otherwise rendering it ineffective.
- Virus protection should facilitate cleaning infected files, not just notification of infection.

Implementation Guideline 3: Implement monitoring and filtering tools in a manner consistent with security policies.

Monitoring and filtering tools are used to implement security policy. They must be checked against this policy to ensure correct implementation.

10.5 Security Audit Standards

Standard 1: Firewall Technology

Agencies with external connection using TCP/IP must utilize firewall technology to protect data and information assets from unauthorized use.

Standard 2: Firewall Testing

Each Agency must test its firewall technology on a periodic basis to ensure compliance with security policies.

Standard 3: Multi-layered Protection
Each Agency must deploy multi-layered protection at the Internet gateway, the network server and the desktop levels to prevent the introduction of malicious code into the State's systems.

Standard 4: Threat Evaluation
Each Agency must establish and implement a process to identify and evaluate threats and assign appropriate action based on severity of risks.

Standard 5: Activity Logging
Firewall technologies must have security logging turned on.

Standard 6: Configuration Management
Each Agency must include a configuration management process in their security program that establishes accountability for changes to information systems components.

Standard 7: Activity Monitoring
Each Agency must monitor and track systems, activities and operations, with resulting data made accessible, to ensure compliance and accountability with security policies.

There are currently no industry-accepted standards for auditing distributed systems. The CIO Council appointed committees will cover standards used to help audit components of the information infrastructure (e.g., SNMP, CMIP, RMON, etc.).

Appendix A - IT Security Principles and Best Practices Summary

General

- Principle 1: Security levels applied to resources should be commensurate to their value to the organization and sufficient to contain risk to an acceptable level.
- Principle 2: The architecture must accommodate varying security needs.
- Principle 3: The architecture must provide integrated security services to enable the enterprise to conduct safe and secure business electronically.
- Principle 4: A single, accurate and consistent system date and time should be maintained across the enterprise.

- Best Practice 1: Perform a business driven risk assessment for all automated systems.
- Best Practice 2: Design application security to follow the State security architecture.
- Best Practice 3: Locate security in the architecture to ensure maximum usability with minimum future modifications.
- Best Practice 4: Develop and implement a security awareness program.
- Best Practice 5: Manage security policies centrally.

Identification

- Best Practice 1: Use risk management techniques when considering biometric identification.
- Best Practice 2: Make user-IDs unique within an agency.
- Best Practice 3: Include user-ID policies in password policies.
- Best Practice 4: Leverage existing technology infrastructure (i.e. ODN – Security Dynamics) when using proprietary tokens.
- Best Practice 5: Use risk management techniques when considering smart cards.

Authentication

- Best Practice 1: Authenticate users prior to accessing private system resources or services.
- Best Practice 2: Use Public Key Infrastructure for authentication when digital signatures are required.
- Best Practice 3: Use an enterprise-wide Public Key Infrastructure (when available).
- Best Practice 4: Use token-based or strong password-based authentication where public key certificates are not feasible, and a high degree of security is require

Authorization and Access Control

- Best Practice 1: Authorize users based on least privilege.
- Best Practice 2: Define appropriate security levels and use these levels for each segment
- of the infrastructure to minimize security management in response to changes.
- Best Practice 3: Use open standards-based security solutions.
- Best Practice 4: Involve security team in the process of selecting protocols.

Administration

- Best Practice 1: Employ a security model that simplifies administration and is easy to maintain.
- Best Practice 2: Use a role-based administration model.
- Best Practice 3: Develop, document, and promote platform-specific standards, best practices, processes, and procedures (e.g. naming standards, addressing standards, procedures to change a user's last name).
- Best Practice 4: Purchase or develop automated administrative tools to ease administration and reduce complexity.
- Best Practice 5: Plan for security when developing applications.
- Best Practice 6: Create an organizational structure with defined and documented security roles and responsibilities.
- Best Practice 7: Provide a strong training program for systems administrators.

Audit

- Best Practice 1: Audit security processes as well as security events (authentication, access, attempted access, etc.).
- Best Practice 2: Audit security policies as well as processes and events.
- Best Practice 3: Use risk management techniques to determine which systems and resources should be monitored.
- Best Practice 4: Agencies should have defined, documented, and tested procedures for responding to attacks (e.g. unauthorized access, denial of service, virus infection.)

Appendix B - Acknowledgements

This document is a joint effort of many Arizona State agencies. It leverages IT architecture work and documentation completed by the states North Carolina, Virginia and Ohio along with research provided earlier by the Gartner Group, GIGA Group and the META Corporation. Work done by the new Federal Homeland Security Agency, US Department of Defense and the State Department are also included for consideration. Additional information about this document and other technology components of the Arizona IT Architecture can be found at the web site:
URL: http://www.gita.state.az.us/

Appendix C - Acronyms / Glossary of Terms

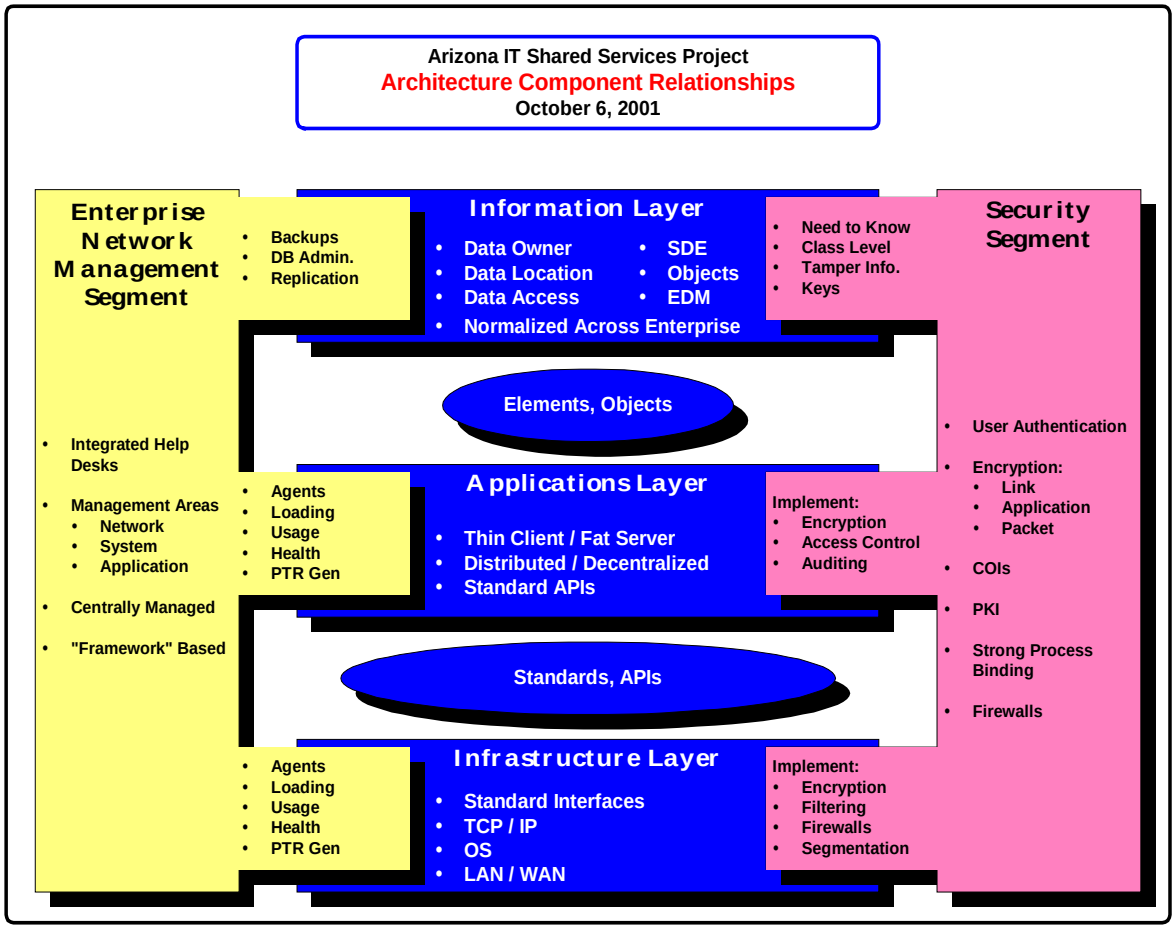
Term	Meaning
Agency	The term "Agency" means executive branch agencies, boards and /or commissions created by the legislature to administer and execute the legitimate functions of government.
API	Application Program Interface
Authentication	The term "authentication" refers to the process of verifying the identity of a user.
Authorization	The term "authorization' refers to the process of establishing and enforcing a user's rights and privileges to access specified computing resources and information.
Bandwidth	Term used to identify, or "measure" the capacity of a telecommunications circuit or local area network (LAN)
CERT	Computer Emergency Response Team
CIMT	Computer Incident Management Team
CISA	Certified Information Systems Auditor
CISSP	Certified Information systems Security Professional
CM	Configuration Management
Critical – or (Mission Critical)	The term "critical" refers to those information resources whose unavailability or improper use has the potential to adversely affect the ability of an Agency to accomplish its mission.
COE	Common Operating Environment. A term used to refer to a specific configuration for platforms such that all users utilize the same configuration thereby lowering management and troubleshooting effort and costs.
COI	Communities of Interest. In the context of this document, this term refers to a set of information, and the users, to which a group of users needs access. This concept is an extension of "need to know".
Data	The term "data" includes but is not limited to data in a database, information about an OS, operational policies and procedures, systems design, organizational policies and procedures, system status, and personal schedules.
DNSSEC	Domain Name System Security
Emerging	One of four categories used in the security domain architecture to guide technology use in Arizona. "Emerging" infers that the State Enterprise Architecture promotes only evaluative deployments of this technology. This technology may be in development or may require evaluation in government and educational settings.

Term	Meaning
Encryption	The use of electronic coding techniques to protect information from disclosure to unauthorized readers, to prevent undetected modification of the information, and to support reader to writer identification and authentication.
FGAC	Fine-grained Access Control
Firewall	Any telecommunication or network device used to regulate / control the flow of information packets between networks. The firewall, or firewalls, implement an IT security policy by screening packets to verify they comply with policy, do not contain malicious code, and are not otherwise attempting to intrude on the protected network side or disrupt its operation.
FTP	File Transfer Protocol
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IDS	Intrusion Detection System
III	Integrated Information Infrastructure
Information	The term “information” means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, images, or audiovisual forms.
Intranet	An internal IP network
IP	Internet Protocol – the basic standard established for data exchange over the worldwide Internet and widely adopted by organizations operating private networks.
IPsec	Internet Protocol Security
ISSO	Information Systems Security Officer
LAN	Local Area Network – a small network that serves a group of users. Typically confined to a single facility.
MAGNET	Arizona State Government Metropolitan Area Government Network that connects the various agencies electronically on the Phoenix Capital Mall and the main campus in Tucson.
NIPRNET	Non Secure Internet Protocol Routed Network
NIST	National Institute of Technology
Obsolescent	One of four categories used in the security domain architecture to guide State technology use (see also emerging, strategic and transitional). “Obsolescent” infers that the Enterprise Architecture actively promotes that agencies employ a different technology. Agencies should not plan new deployments of this technology. Agencies should develop plans to replace this technology.

Term	Meaning
OS	Operating System
OSI	Open System Interconnect
Owner	The term "owner' refers to that group which controls a set of information resources and determines its level of criticality and sensitivity. As such, they determine access, authorization rights, and dissemination regarding those resources.
PGP	Pretty Good Privacy (a security product name)
PKI	Public Key Infrastructure. The term used to refer the system required to supply and manage certificates for public key encryption and digital signature used by clients and servers to authenticate customers as valid.
Platform	In the context of this document, the platform is the stable, cross-project base of both hardware and infrastructure software provided to (and evolved for) all projects.
Policy	The term policy means any general statement of direction and purpose designed to promote the coordinated planning, practical acquisition, effective development, and efficient use of information technology resources.
Protocol	A defined structure, content, and flow for communications between computers and other networked devices.
S/MIME	Secure/Multipurpose Internet Mail Extension. Provides a consistent way to exchange secure MIME data. Based on the popular Internet MIME standard, S/MIME provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption). S/MIME is used by traditional mail user agents to secure text and attachments. However, S/MIME is not restricted to mail: it can be used with any transport protocol that transports MIME data, such as HTTP. As such, S/MIME takes advantage of the object-based features of MIME and allows secure messages to be exchanged in mixed-transport systems. Further, S/MIME can be used in automated message transfer agents that use cryptographic security services that do not require any human intervention, such as the signing of software-generated documents and the encryption of FAX messages sent over the Internet.
SDE	Standard Data Element
SHTTP	Secure Hypertext Transfer Protocol. A means of securely transmitting HTTP formatted information.
SIG	State Information Grid
SIPRNET	Secure Internet Protocol Routed Network
SLA	Service Level Agreement – a definition of the type, quality, and quantity of network services agreed to by the provider and customer.

Term	Meaning
SSH	Secure Shell Protocol
SSL	Secure Socket Layer - A means of securely transmitting web pages.
Standard	Agreement on the rules, procedures, and content of AIS and telecommunications exchange to include open standards, industry standards and de facto standards.
Strategic	One of four categories used in the security domain architecture to guide technology use in the State. (see also emerging, obsolescent, and transitional) "Strategic' infers that the Enterprise Architecture promotes use of this technology by agencies. New deployments of this technology are recommended.
TCP/IP	Transmission Control Protocol / Internet Protocol
Thin Client	In the context of this document, "thin client" refers to minimizing the amount of processing logic and data manipulation on a client to the maximum extent possible.
Transitional	One of four categories used in the security domain architecture to guide technology use in the State (see also emerging, obsolescent and strategic) "Transitional" infers that the State Enterprise Architecture promotes other standard technologies. Agencies may be using this technology as a transitional strategy in movement to a more strategic technology. This technology may be waning in use or no longer supported.
User	An individual or group who has access to an information system or its data.
VPN	Virtual Private Network – a capability to split a physical network or circuit path into two or more sub-paths that use various protocols to define the circuit path and protect the data from tampering.
WAN	Wide Area Network – This refers to a collection of circuits that interconnect a widely dispersed set of facilities, and other networks
X.500	A CCITT protocol, X.500 is a family of standards and uses a distributed approach to realize a global directory service. Information of an organization is maintained in one or more so-called directory system agendas (DSAs). The X.500 directory supports a variety of services including security (certificates), e-mail (addressing), and "white pages" (name and phone number)
X.509	One of the X.500 standards that defines a security certificate to provide a vehicle for associating users with their encryption keys. All of the user's "public" information is stored in a X.509 certificate for use when exchanging information securely with that user. Other information such as to whom does the user belong, what authority issued the keys, when do the keys expire, what levels of information classification is this user allowed to access, and how can the certificate be validated is also included.

Appendix D – Architecture Component Relationships Diagram



Appendix E - Security Domain Team Members and Support Staff

Security Domain Team Members

(to be organized)

Name	Title	Agency
Lee Lane	Information Systems Security Officer	ADOA
Rupert Loza	Manager	GITA
Russ Savage	IT Consultant – PKI Security Requirements	SOS
To be named		DES
"		DOT
"		AHCCCS
"		DEQ
"		DOR
"		Other
"		Other

It is recommended that, through the CIO Council, a task team be named to take the "straw-man" draft security architecture contained in this document and evolve it into the final product for the State of Arizona. Any agency that would like to assist in the development of this architecture should not be excluded from participating.

Security Domain Support Staff

Name	Title	Agency
John McDowell	Chief Technology Planner	ADOA
Gerald L. Rinehart	IT Executive Consultant	ADOA
Bob Brewer	IT Security Analyst	ADOA
To be named		GITA